

One-Way Reversible and Quantum Finite Automata with Advice*

TOMOYUKI YAMAKAMI[†]

Abstract: We examine characteristic features of reversible and quantum computations in the presence of supplementary external information, known as advice. In particular, we present a simple, algebraic characterization of languages recognized by one-way reversible finite automata augmented with deterministic advice. With a further elaborate argument, we prove a similar but slightly weaker result for bounded-error one-way quantum finite automata with advice. An immediate application of those properties leads to containments and separations among various language families that are further assisted by appropriate advice. We further demonstrate the power of randomized advice and quantum advice when given to one-way quantum finite automata.

Keywords: reversible finite automaton, quantum finite automaton, regular language, context-free language, randomized advice, quantum advice

1 Background, Motivations, and Challenges

From theoretical and practical interests, we wish to promote our basic understandings of the exotic behaviors of reversible and quantum computations by examining machine models of those computations, in particular, two weak models, known as reversible finite automata and quantum finite automata. Of various types of such automata, in order to make our argument clear and transparent, we initiate our study by limiting our focal point within one of the simplest automaton models: *one-way deterministic reversible finite automata* (or 1rfa's, in short) and *one-way measure-many quantum finite automata* (or 1qfa's, thereafter). Our 1qfa scans each read-only input tape cell by moving a single tape head only in one direction (without stopping) and performs a (*projection*) *measurement* immediately after every head move, until the tape head scans the right endmarker. From a theoretical perspective, the 1qfa's with more than $7/9$ success probability are essentially as powerful as 1rfa's [2], and therefore 1rfa's are important part of 1qfa's. Notice that, for bounded-error 1qfa's, it is not always possible to make a sufficient amplification of success probability. This is one of many features that make an analysis of 1qfa's quite different from that of polynomial-time quantum Turing machines. These intriguing features of 1qfa's, on the contrary, have kept stimulating our research since their introduction in late 1990s. Back in an early period of intensive study, numerous unconventional features have been revealed. For instance, as Ambainis and Freivalds [2] demonstrated, certain quantum finite automata can be built more state-efficiently than deterministic finite automata. However, as Kondacs and Watrous [7] proved, a certain regular language cannot be recognized by any 1qfa with bounded-error probability. Moreover, by Brodsky and Pippenger [4], no bounded-error 1qfa recognizes languages accepted by minimal finite automata that lack a so-called *partial order condition*. The latter two facts suggest that the language-recognition power of 1qfa's is hampered by their own inability to generate useful quantum states from input information. To overcome such drawbacks, a simple, straightforward way is to appeal to an outside information source.

In a wide range of literature, various notions of classical machines equipped with supplemental information have been extensively studied. Because of its simplicity, we consider Karp and Lipton's [6] style of information, known as (*deterministic*) *advice*, a piece of which encodes additional data, given in parallel with a standard input, into a single string (called an *advice string*) depending only on the size of the input. A series of recent studies [13, 14, 15, 16] on classical one-way finite automata that process such advice have unearthed advice's delicate roles. These advised automaton models have immediate connections to other fields, including one-way communication, random access coding, and two-player zero-sum games. Two central questions concerning the advice are: how can we encode necessary information into a piece of advice before a computation starts and, as a computation proceeds step by step, how can we decode and utilize such information stored inside the advice?

*An extended abstract appeared in the Proceedings of the 6th International Conference on Language and Automata Theory and Applications (LATA 2012), March 5–9, 2012, A Coruña, Spain, Lecture Notes in Computer Science, Springer-Verlag, Vol.7183, pp.526–537, 2012. This work was partly supported by the Mazda Foundation and the Japanese Ministry of Education, Science, Sports, and Culture.

[†]Affiliation: Department of Information Science, University of Fukui, 3-9-1 Bunkyo, Fukui 910-8507, Japan

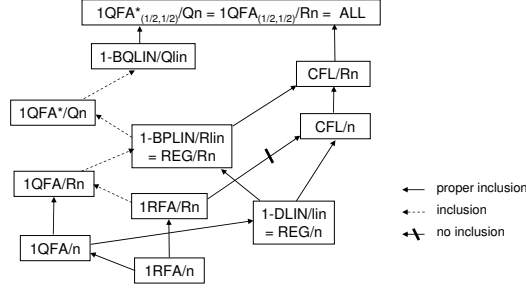


Figure 1: A hierarchy of advised language families. All containments and separations associated with quantum finite automata, reversible automata, and quantum Turing machines are newly proven in this paper.

As for a model of polynomial-time quantum Turing machine, there is a rich literature on the power and limitation of advice (see, for instance, [1, 10, 12]); disappointingly, little is known for the roles of advice when it is given to finite automata, in particular, 1rfa’s and 1qfa’s. For bounded-error 1qfa’s, for instance, an immediate advantage of taking such advice is the elimination of both endmarkers placed on a read-only input tape. Beyond such an obvious advantage, however, there are numerous challenges in the study of the roles of advice. The presence of advice tends to make an analysis of underlying computations quite difficult and it often demands quite different kinds of proof techniques. As a quick example, a standard *pumping lemma*—a typical proof technique that showcases the non-regularity of a given language—is not quite serviceable to advised computations; therefore, we need to develop other tools (e.g., a swapping lemma [14]) for them. In a similar light, certain advised 1qfa’s violate the aforementioned criterion of the partial order condition (see Section 3.1), and this fact makes a proof technique of [7] inapplicable to, for example, a class separation between regular languages and languages accepted by bounded-error advised 1qfa’s.

To analyze the behaviors of advised 1qfa’s as well as advised 1rfa’s, we face numerous challenges. Our first task is to lay out a necessary ground work in order to (1) capture the fundamental features of those automata when advice is given to boost their language-recognition power and (2) develop methodology necessary to lead to collapses and separations of advised language families. In particular, the aforementioned difficulties surrounding the advice for 1qfa’s motivate us to seek different kinds of proof techniques.

In Sections 3.2 and 4, we will prove two main theorems. As the first main theorem (Theorem 3.4), with an elaborate argument, we will show a machine-independent, algebraic sufficient condition for languages to be recognized by bounded-error 1qfa’s that take appropriate deterministic advice. For 1rfa’s augmented with deterministic advice, we will give a machine-independent, algebraic necessary and sufficient condition as the second theorem (Theorem 4.1). These two conditions exhibit certain behavioral characteristics of 1rfa’s and 1qfa’s when appropriate advice is provided. Our proof techniques for 1qfa’s, for instance, are quite different from the previous work [2, 3, 4, 7, 8]. Applying these theorems further, we can prove several class separations among advised language families. These separations indicate, to some extent, inherent strengths and weaknesses of reversible and quantum computations even in the presence of advice.

Another quick benefit of the theorems is a revelation of the excessive power of *randomized advice* over deterministic advice in the field of reversible and quantum computation. In randomized advice, advice strings of a fixed length are generated at random according to a pre-determined probability distribution so that a finite automaton “probabilistically” processes those generated advice strings. *Quantum advice* further extends randomized advice; however, the aforementioned model of 1qfa with “read-only” advice strings inherently has a structural limitation that prevents quantum advice from being more resourceful than randomized advice. Another challenging task we engage in throughout Section 5.2 is to seek a simple modulation of the 1qfa’s in order to utilize quantum information stored in quantum advice more effectively. We will discuss in Section 5.2 how to remedy the deficiency of the current model of 1qfa and direct implications of such a remedy.

A Quick Overview of Relations among Advised Language Families: As summarized in Fig. 1, we obtain new containments and separations of new advised language families in direct comparison with existing classical advised language families. Our main theorems are particularly focused on two language families: the family 1RFA of all languages accepted by 1rfa’s and the family 1QFA of languages recognized by 1qfa’s with bounded-error probability. Associated with these language families, we will introduce their corresponding

advised language families[‡]: $1\text{RFA}/n$, $1\text{RFA}/Rn$, $1\text{QFA}/n$, $1\text{QFA}/Rn$, and $1\text{QFA}^*/Qn$, except that $1\text{QFA}^*/Qn$ uses a slightly relaxed 1qfa model[§] discussed earlier. In Fig. 1, “ALL” indicates the collection of all languages. Language families REG (regular) and CFL (context-free) are based on classical one-way finite automata. Moreover, language families 1-DLIN (deterministic), 1-BPLIN (bounded-error probabilistic), and 1-BQLIN (bounded-error quantum) [13], which are viewed respectively as “scaled-down” versions of the well-known complexity classes P, BPP, and BQP, are based on the models of one-tape one-head two-way off-line Turing machines running in “linear time,” in the sense of a so-called *strong definition* of running time (see [9, 13]). Supplementing various types of advice to those families introduces the following advised language families: REG/n , CFL/n , REG/Rn , CFL/Rn , $1\text{-DLIN}/lin$, $1\text{-BPLIN}/lin$, $1\text{-BPLIN}/Rlin$ [13, 14, 15], and $1\text{-BQLIN}/Qlin$. The reader may refer to [13, 16] for other advice language families not listed in Fig. 1.

2 Basic Terminology

We briefly explain fundamental notions and notations used in this paper. First, we write \mathbb{N} for the set of all *natural numbers* (i.e., nonnegative integers). An *integer interval* $[m, n]_{\mathbb{Z}}$ is the set $\{m, m+1, m+2, \dots, n\}$ for any pair $m, n \in \mathbb{N}$ with $m \leq n$. We abbreviate $[1, n]_{\mathbb{Z}}$ as $[n]$ if $n \geq 1$. In addition, we denote by \mathbb{R} and \mathbb{C} respectively the sets of all *real numbers* and of all *complex numbers*. An *alphabet* Σ is a finite nonempty set and a *string* over Σ is a finite sequence of symbols taken from Σ . In particular, the *empty string* is always denoted λ and we use the notation Σ^+ for $\Sigma^* - \{\lambda\}$. The *length* $|x|$ of a string x is the total number of symbols in x . The notation Σ^n indicates the set of all strings, over Σ , of length exactly n . For any string x and any number $n \in \mathbb{N}$, $\text{Pref}_n(x)$ expresses the string consisting of the first n symbols of x when $n \leq |x|$. In particular, $\text{Pref}_0(x)$ equals λ . A *language* over Σ is a subset of Σ^* . We conveniently identify a language L with its *characteristic function*, which is defined as $L(x) = 1$ (resp., $L(x) = 0$) if $x \in L$ (resp., $x \notin L$). Given an alphabet Γ , a *probability ensemble* over Γ^* refers to an infinite series $\{D_n\}_{n \in \mathbb{N}}$ of probability distributions, in which each D_n maps Γ^n to the unit real interval $[0, 1]$. Let REG, CFL, and DCFL denote respectively the families of *regular languages*, of *context-free languages*, and of *deterministic context-free languages*. We abbreviate as *1dfa* (resp., *1npda*) a one-way deterministic finite automaton (resp., one-way nondeterministic pushdown automaton). For ease of our later analysis, we explicitly assume, unless otherwise stated, that (1) every finite automaton is equipped with a single read-only input tape on which each input string is initially surrounded by two endmarkers (the left endmarker ϵ and the right endmarker $\$$), (2) every finite automaton has a single tape head that is initially situated at the left endmarker, and (3) every finite automaton moves its tape head rightward without stopping until it scans the right endmarker. For a later reference, we formally define a 1dfa as a sextuple $M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$, where Q is a finite set of inner states, Σ is an input alphabet, $\delta : Q \times \tilde{\Sigma} \rightarrow Q$ is a transition function, $q_0 (\in Q)$ is the initial state, $Q_{acc} (\subseteq Q)$ is a set of accepting states, and $Q_{rej} (\subseteq Q - Q_{acc})$ is a set of rejecting states, where $\tilde{\Sigma}$ denotes the set $\Sigma \cup \{\epsilon, \$\}$ of tape symbols. For convenience, we also set $Q_{halt} = Q_{acc} \cup Q_{rej}$ and $Q_{non} = Q - Q_{halt}$. An *extended transition function* induced from δ is defined as $\hat{\delta}(q, \lambda) = q$ and $\hat{\delta}(q, x\sigma) = \delta(\hat{\delta}(q, x), \sigma)$ for any $x \in \Sigma^*$ and $\sigma \in \Sigma$.

To introduce a notion of (*deterministic*) *advice* that is fed to finite automata beside input strings, we adopt the “track” notation of [13]. For two symbols $\sigma \in \Sigma$ and $\tau \in \Gamma$, where Σ and Γ are two alphabets, the notation $[\begin{smallmatrix} \sigma \\ \tau \end{smallmatrix}]$ expresses a new symbol made up of σ and τ . Graphically, this new symbol is written on an input tape cell, which is split into two tracks whose upper track contains σ and lower track contains τ . Since the symbol $[\begin{smallmatrix} \sigma \\ \tau \end{smallmatrix}]$ is in one tape cell, a tape head scans the two track symbols σ and τ simultaneously. When two strings x and y are of the same length n , the notation $[\begin{smallmatrix} x \\ y \end{smallmatrix}]$ denotes a concatenated string $[\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}][\begin{smallmatrix} x_2 \\ y_2 \end{smallmatrix}] \dots [\begin{smallmatrix} x_n \\ y_n \end{smallmatrix}]$, provided that $x = x_1x_2 \dots x_n \in \Sigma^n$ and $y = y_1y_2 \dots y_n \in \Gamma^n$. Using this track notation, we define Σ_{Γ} to be a new alphabet $\{[\begin{smallmatrix} \sigma \\ \tau \end{smallmatrix}]\mid \sigma \in \Sigma, \tau \in \Gamma\}$ induced from two alphabets Σ and Γ . An *advice function* h is a function mapping \mathbb{N} to Γ^* , where Γ is an *advice alphabet*, but h is not required to be “computable.” The advised language family REG/n of Tadaki, Yamakami, and Lin [13] is the family of all languages L over certain alphabets Σ satisfying the following condition: there exist a 1dfa M , an advice alphabet Γ , and an advice function $h : \mathbb{N} \rightarrow \Gamma^*$ for which (i) for every length $n \in \mathbb{N}$, $|h(n)| = n$ holds and (ii) for every string $x \in \Sigma^*$, $x \in L$ iff M accepts the input $[\begin{smallmatrix} x \\ h(|x|) \end{smallmatrix}]$. Similarly, CFL/n is defined in [14, 15] using 1npda’s in place of 1dfa’s.

[‡]To clarify the types of advice, we generally use the following specific suffixes. The suffixes “/n” and “/Rn” respectively indicate a use of deterministic advice and randomized advice of input size, whereas “/lin” and “/Rlin” respectively indicate a use of deterministic advice and randomized advice of linear size. Similarly, “/Qn” and “/Qlin” indicate the use of quantum advice of input size and of linear size.

[§]Such a relaxation does not affect classical advice families, e.g., $\text{REG}^*/n = \text{REG}/n$ holds.

3 Properties of Advice for Quantum Computation

Since its introduction by Karp and Lipton [6], the usefulness of advice has been demonstrated for various models of underlying computations. Following this line of study, we begin with examining characteristic features of a quantum language family that is assisted by powerful pieces of advice.

In particular, we will examine *one-way measure-many quantum finite automata* (or 1qfa's, in short) that process deterministic advice with bounded-error probability, where every 1qfa permits only one-way head moves and performs a (projection) measurement, at each step, to see if the machine enters any halting state (i.e., either an accepting state or a rejecting state).

3.1 Basic Properties of 1QFA/ n

Formally, a 1qfa M is defined as a sextuple $(Q, \Sigma, \{U_\sigma\}_{\sigma \in \tilde{\Sigma}}, q_0, Q_{acc}, Q_{rej})$, where each *time-evolution operator* U_σ is a unitary operator acting on the Hilbert space $E_Q = \text{span}\{|q\rangle \mid q \in Q\}$ of dimension $|Q|$. Recall that $\tilde{\Sigma} = \Sigma \cup \{\$, \#\}$. The series $\{U_\sigma\}_{\sigma \in \tilde{\Sigma}}$ describe the *time evolution* of M , where each U_σ is a unitary operator acting on E_Q . Let P_{acc} , P_{rej} , and P_{non} be respectively the projections of E_Q onto the subspaces $E_{acc} = \text{span}\{|q\rangle \mid q \in Q_{acc}\}$, $E_{rej} = \text{span}\{|q\rangle \mid q \in Q_{rej}\}$, and $E_{non} = \text{span}\{|q\rangle \mid q \in Q_{non}\}$. Associated with a symbol $\sigma \in \tilde{\Sigma}$, we define a *transition operator* T_σ as $T_\sigma = P_{non}U_\sigma$. For each fixed string $x = \sigma_1\sigma_2 \cdots \sigma_n$ in $\tilde{\Sigma}^*$, we set $T_x = T_{\sigma_n}T_{\sigma_{n-1}} \cdots T_{\sigma_2}T_{\sigma_1}$.

To describe precisely the *time-evolution* of M , let us consider a new Hilbert space \mathcal{S} spanned by the basis vectors of $E_Q \times \mathbb{R} \times \mathbb{R}$. We then define a *norm*[¶] of an element $\psi = (|\phi\rangle, \gamma_1, \gamma_2)$ in \mathcal{S} to be $\|\psi\| = (\|\phi\|^2 + |\gamma_1| + |\gamma_2|)^{1/2}$. For this space \mathcal{S} , we extend the aforementioned transition operator T_σ to \hat{T}_σ by setting $\hat{T}_\sigma(|\phi\rangle, \gamma_1, \gamma_2) = (T_\sigma|\phi\rangle, \gamma_1 + \|P_{acc}U_\sigma|\phi\rangle\|^2, \gamma_2 + \|P_{rej}U_\sigma|\phi\rangle\|^2)$. Given an arbitrary string $x = \sigma_1\sigma_2 \cdots \sigma_n$ in $\tilde{\Sigma}^*$, we further define \hat{T}_x as $\hat{T}_{\sigma_n}\hat{T}_{\sigma_{n-1}} \cdots \hat{T}_{\sigma_1}$. Notice that this extended operator \hat{T}_x may not be a linear operator in general; however, it satisfies useful properties listed in Lemma 3.1, which will play a key role in the proof of Theorem 3.4. To improve readability, we place in Appendix the proof of this lemma.

Lemma 3.1 *Let $x \in \tilde{\Sigma}^*$ be any string. Moreover, let ψ and ψ' be two elements in \mathcal{S} and let $|\phi\rangle$ and $|\phi'\rangle$ be two quantum states in E_{non} . Each of the following statements holds.*

1. $\| |\phi\rangle - |\phi'\rangle \|^2 - \| T_x(|\phi\rangle - |\phi'\rangle) \|^2 \leq 2[(\|\phi\|^2 - \|T_x|\phi\rangle\|^2) + (\|\phi'\|^2 - \|T_x|\phi'\rangle\|^2)]$.
2. $\|\psi + \psi'\| \leq \|\psi\| + \|\psi'\|$.
3. $\|\hat{T}_x\psi - \hat{T}_x\psi'\| \leq \sqrt{2}\|\psi - \psi'\|$.
4. *If $\psi = (|\phi\rangle, \gamma_1, \gamma_2)$ and $\psi' = (|\phi'\rangle, \gamma'_1, \gamma'_2)$, then $\|\hat{T}_x\psi - \hat{T}_x\psi'\|^2 \geq \|\psi - \psi'\|^2 - 3(\|\phi\rangle - |\phi'\rangle\|^2 - \|T_x(|\phi\rangle - |\phi'\rangle)\|^2)$.*

A length- n input string x given to the 1qfa M must be expressed on an input tape in the form $\#x\$ = \sigma_1\sigma_2 \cdots \sigma_{n+2}$, including the two endmarkers $\#$ and $\$$; in other words, $\sigma_1 = \#$, $\sigma_{n+2} = \$$, and $x \in \Sigma^n$. The *acceptance probability* of M on the input x at step i ($1 \leq i \leq n+2$), denoted $p_{acc}(x, i)$, is $\|P_{acc}U_{\sigma_i}|\phi_{i-1}\rangle\|^2$, where $|\phi_0\rangle = |q_0\rangle$ and $|\phi_i\rangle = T_{\sigma_i}|\phi_{i-1}\rangle$, and the *acceptance probability* of M on x , denoted $p_{acc}(x)$, is $\sum_{i=1}^{n+2} p_{acc}(x, i)$. Similarly, we define the *rejection probabilities* $p_{rej}(x, i)$ and $p_{rej}(x)$ using P_{rej} instead of P_{acc} in the above definition. The 1qfa M must halt after the $n+2$ nd step. In the end of a computation of M on x , M produces an element $\hat{T}_{\#x\$}(|q_0\rangle, 0, 0) = (|\phi_{n+2}\rangle, p_{acc}(x), p_{rej}(x))$. Conventionally, we say that M accepts (resp., rejects) x with probability $p_{acc}(x)$ (resp., $p_{rej}(x)$).

Regarding language recognition, we say that a language L is *recognized* by a 1qfa M with *error probability* ε if (i) for every string $x \in L$, M accepts x with probability at least $1 - \varepsilon$ and (ii) for every string $x \in \Sigma^* - L$, M rejects with probability at least $1 - \varepsilon$. By viewing M as a machine outputting two values, 0 (rejection) and 1 (acceptance), Conditions (i) and (ii) can be rephrased succinctly as follows: for every string $x \in \Sigma^*$, M on the input x outputs $L(x)$ with probability at least $1 - \varepsilon$.

The notation 1QFA denotes the family of all languages recognized by 1qfa's with *bounded-error probability* (i.e., the error probability is upper-bounded by an absolute constant in the real interval $[0, 1/2)$). For latter use, we also introduce the notation $1QFA_{(a(n), b(n))}$ defined as follows. For any two functions $a(n)$ and $b(n)$ mapping \mathbb{N} to $[0, 1]$, $1QFA_{(a(n), b(n))}$ denotes the collection of all languages L such that there exists a 1qfa M satisfying: for every length $n \in \mathbb{N}$ and every input $x \in \Sigma^n$, if $x \in L$ then M accepts x with probability more than $a(n)$, and if $x \notin L$ then M rejects x with probability more than $b(n)$.

[¶]Our definition of "norm" is slightly different in its form from the norm defined in [7].

Naturally, we can supply (deterministic) advice to 1qfa's. Similar to 1RFA/ n , the notation 1QFA/ n indicates the collection of all languages L over alphabets Σ that satisfy the following condition: there exist a 1qfa M , an error bound $\varepsilon \in [0, 1/2)$, an advice alphabet Γ , and an advice function $h : \mathbb{N} \rightarrow \Gamma^*$ such that (i) $|h(n)| = n$ for each length $n \in \mathbb{N}$ and (ii) for every $x \in \Sigma^*$, M on input $[h(\frac{x}{|x|})]$ outputs $L(x)$ with probability at least $1 - \varepsilon$ (abbreviated as $\text{Prob}_M[M([h(\frac{x}{|x|})]) = L(x)] \geq 1 - \varepsilon$), where $M([h(\frac{x}{|x|})])$ is seen as a random variable. Similar to a known inclusion $1\text{QFA} \subseteq \text{REG}$ [7], $1\text{QFA}/n \subseteq \text{REG}/n$ holds by examining how advice is provided to underlying quantum finite automata.

An immediate benefit of supplementing 1qfa's with appropriate advice is the elimination of endmarkers on their input tapes. Earlier, Brodsky and Pippenger [4] demonstrated that we can eliminate the left endmarker $\$$ from 1qfa's. The use of advice further enables us to eliminate the right endmarker $\$$ as well. Intuitively, this elimination is done by marking the end of an input string by a piece of advice.

Lemma 3.2 [endmarker lemma] *For any language L in 1QFA/ n , there exist a 1qfa M , a constant $\varepsilon \in [0, 1/2)$, an advice alphabet Γ , and an advice function h such that (i) M 's input tape has no endmarkers, (ii) $|h(n)| = n$ holds for any length $n \in \mathbb{N}$, and (iii) $\text{Prob}_M[M([h(\frac{x}{|x|})]) = L(x)] \geq 1 - \varepsilon$ holds for any input string $x \in \Sigma^*$.*

Proof. Let L be any language in 1QFA/ n over alphabet Σ . Associated with this L , we take an advice function $h : \mathbb{N} \rightarrow \Gamma^*$ with an advice alphabet Γ and a 1qfa $M = (Q, \Sigma_\Gamma, \{U_\sigma\}_{\sigma \in \Sigma_\Gamma}, q_0, Q_{acc}, Q_{rej})$. Here, we assume that, for any string $x \in \Sigma^*$, M on input of the form $[h(\frac{x}{|x|})]$ outputs $L(x)$ with probability at least $1 - \varepsilon$. For convenience, assume that $Q_{non} = \{q_i \mid 1 \leq i \leq k_0\}$, $Q_{acc} = \{q_{k_0+i} \mid 1 \leq i \leq k_1\}$, and $Q_{rej} = \{q_{k_0+k_1+i} \mid 1 \leq i \leq k_2\}$, where $k_0, k_1, k_2 \in \mathbb{N}^+$. We therefore set $Q = Q_{non} \cup Q_{acc} \cup Q_{rej}$ and let $k = |Q|$. Following an argument of Brodsky and Pippenger [4], we can eliminate the left endmarker $\$$, and hereafter we assume that M 's input tape has no $\$$.

In the following manner, we will modify M and h . Let us assume that h has the form $h(n) = \tau_1 \cdots \tau_{n-1} \tau_n$. A new advice function h' is defined to satisfy $h'(n) = \tau_1 \cdots \tau_{n-1} \tau'_n$, where the last symbol τ'_n is $[\frac{\tau_n}{\$}]$, indicating the end of input strings of length n . To describe a new 1qfa M' , we want to embed each operator U_σ into a slightly larger space, say, $E_{Q'}$. For this purpose, we first define $Q'_{acc} = \{q_{k+i} \mid 1 \leq i \leq k_1\}$ and $Q'_{rej} = \{q_{k+k_1+i} \mid 1 \leq i \leq k_2\}$, and we then set $Q' = Q \cup Q'_{acc} \cup Q'_{rej}$. To describe new operators, we need a special unitary matrix S , which is called "sweeping" matrix in [4]. This matrix S is defined as

$$S = \begin{pmatrix} I_{non} & O & O \\ O & O & I_{halt} \\ O & I_{halt} & O \end{pmatrix},$$

where I_{non} (resp., I_{halt}) is the identity matrix of size k_0 (resp., $k_1 + k_2$). This matrix S swaps "old" halting states of M with "new" non-halting states so that, after an application of unitary matrix $U_{[\frac{\sigma}{\$}]}$, we can deter the effect of an application of the measurement P_{non} that immediately follows $U_{[\frac{\sigma}{\$}]}$. Using this operator S , we further define

$$U'_{[\frac{\sigma}{\$}]} = S \begin{pmatrix} U_{[\frac{\sigma}{\$}]} & O \\ O & I_{halt} \end{pmatrix} \quad \text{and} \quad U'_{[\frac{\sigma}{\$}]} = S \begin{pmatrix} U_{\$} & O \\ O & I_{halt} \end{pmatrix} \begin{pmatrix} U_{[\frac{\sigma}{\$}]} & O \\ O & I_{halt} \end{pmatrix},$$

where $\tau' = [\frac{\tau}{\$}]$. The measurement operator P_{acc} is also expanded naturally to the space $E_{Q'}$, and it is denoted P'_{acc} . It is not difficult to show that the operator $P'_{acc} U'_{[\frac{\sigma}{\$}]}$ produces a similar effect as the operator $P_{acc} U_{\$} P_{non} U_{[\frac{\sigma}{\$}]}$. Therefore, with the advice function h' , M' accepts the input x with the same probability as M does with the advice function h . \square

Toward an analysis of the behaviors of languages in 1QFA/ n , some of the well-known properties proven for 1QFA do not turn out to be as useful as we hope them to be. One such property is a criterion, known as a *partial order condition*^{||} of Brodsky and Pippenger [4]. Earlier, Kondacs and Watrous [7] proved that $\text{REG} \not\subseteq 1\text{QFA}$ by considering a separation language $L_a = \{wa \mid w \in \Sigma^*\}$ over an alphabet $\Sigma = \{a, b\}$. As Brodsky and Pippenger [4] pointed out, this result follows from a more general fact that every language in 1QFA satisfies the partial order condition but L_a does not. Unlike 1QFA, 1QFA/ n violates this criteria because the above language L_a falls into 1QFA/ n . This fact is a typical example that makes an analysis of 1QFA/ n quite different from an analysis of 1QFA.

^{||} A language satisfies the partial order condition exactly when its minimal 1dfa contains no two inner states $q_1, q_2 \in Q$ such that (i) there is a string z for which $\hat{\delta}(q_1, z) \in Q_{acc}$ and $\hat{\delta}(q_2, z) \notin Q_{acc}$ or vice versa, and (ii) there are two nonempty strings x and y for which $\hat{\delta}(q_1, x) = \hat{\delta}(q_2, x) = q_2$ and $\hat{\delta}(q_2, y) = q_1$.

Lemma 3.3 *The advised language family 1QFA/ n does not satisfy the criterion of the partial order condition.*

Proof. Let $\Sigma = \{a, b\}$ and consider the aforementioned language $L_a = \{wa \mid w \in \Sigma^*\}$. We aim at proving that this language belongs to 1QFA/ n by constructing an appropriate 1qfa M and an advice function h . Since L_a does not satisfy the partial order condition, the lemma immediately follows.

It suffices by Lemma 3.2 to build an advised 1qfa without any endmarker. Our advice alphabet Γ is $\{0, 1\}$, and the desired 1qfa M is defined as $(Q, \Sigma_\Gamma, \{U_\sigma\}_{\sigma \in \Sigma_\Gamma}, q_0, Q_{acc}, Q_{rej})$, where $Q = \{q_0, q_1, q_2\}$, $Q_{acc} = \{q_1\}$, and $Q_{rej} = \{q_2\}$. Time-evolution operators of M consist of $U_{[e]} = I$ (identity) for each symbol $e \in \Sigma$ and

$$U_{[1]} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } U_{[b]} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Finally, we set an advice function h to be $h(n) = 0^{n-1}1$, which gives a cue to the 1qfa M to check whether the last input symbol equals a . An initial configuration of M is $|\psi_0\rangle = (1, 0, 0)^T$, indicating that $|q_0\rangle$ has amplitude 1.

A direct calculation shows that $U_{[0^{n-1}1]}|q_0\rangle = |q_1\rangle$ and $U_{[0^{n-1}1]}|q_0\rangle = |q_2\rangle$. Since $q_1 \in Q_{acc}$ and $q_2 \in Q_{rej}$, M should recognize L_a with certainty, leading to the conclusion that L_a belongs to 1QFA/ n , as requested. \square

3.2 A Sufficient Condition for 1QFA/ n

To understand an essence of the computational behaviors of advised 1qfa's, a quick way may be to find a machine-independent, algebraic characterization of languages recognized by those automata using deterministic advice. Such a characterization may turn out to be a useful tool in studying the computational complexity of the languages. What we plan to prove here is a slightly weaker result: a machine-independent, algebraic *sufficient* condition for those languages that fall into 1QFA/ n .

We begin with a precise description of our first main theorem, Theorem 3.4. Following a standard convention, for any partial order \leq defined on a finite set, we use the notation $x = y$ exactly when both $x \leq y$ and $y \leq x$ hold; moreover, we write $x < y$ in the case where both $x \leq y$ and $x \neq y$ hold. With respect to \leq , a finite sequence (s_1, s_2, \dots, s_m) is called a *strictly descending chain* of length m if $s_{i+1} < s_i$ holds for any index $i \in [m-1]$. For our convenience, we call a reflexive, symmetric, binary relation a *closeness relation*. Given a closeness relation \cong , an \cong -*discrepancy set* is a set S satisfying that, for any two elements $x, y \in S$, if x and y are different, then $x \not\cong y$.

Theorem 3.4 *Let S be any language over alphabet Σ and let $\Delta = \{(x, n) \in \Sigma^* \times \mathbb{N} \mid |x| \leq n\}$. If S belongs to 1QFA/ n , then there exist two constants $c, d \in \mathbb{N}^+$, an equivalence relation \equiv_S over Δ , a partial order \leq_S over Δ , and a closeness relation \cong over Δ that satisfy the seven conditions listed below. In the list, we assume that $(x, n), (y, n) \in \Delta$, $z \in \Sigma^*$, and $\sigma \in \Sigma$ with $|x| = |y|$.*

1. *The set Δ/\equiv_S of equivalence classes is finite.*
2. *If $(x, n) \cong (y, n)$, then $(x, n) \equiv_S (y, n)$.*
3. *If $|x\sigma| \leq n$, then $(x\sigma, n) \leq_S (x, n)$.*
4. *If $|xz| \leq n$, $(x, n) =_S (xz, n)$, $(y, n) =_S (yz, n)$, and $(xz, n) \cong (yz, n)$, then $(x, n) \equiv_S (y, n)$.*
5. *$(x, n) \equiv_S (y, n)$ iff $S(xz) = S(yz)$ for all strings $z \in \Sigma^*$ with $|xz| = n$.*
6. *Any strictly descending chain (w.r.t. \leq_S) in Δ has length at most c .*
7. *Any \cong -discrepancy subset of Δ has cardinality at most d .*

The meanings of the above three relations \cong , \leq_S , and \equiv_S will be clarified in the following proof of Theorem 3.4. Since our proof of the theorem heavily depends on Lemma 3.1, the proof requires only basic properties of the norm in the designated Hilbert space \mathcal{S} .

Proof of Theorem 3.4. Let Σ be any alphabet, let $\Delta = \{(x, n) \mid x \in \Sigma^*, |x| \leq n\}$, and let S be any language over Σ in 1QFA/ n . For this language S , there exist an advice alphabet Γ , an error bound $\varepsilon \in [0, 1/2)$, a 1qfa M , and an advice function $h : \mathbb{N} \rightarrow \Gamma^*$ satisfying $\text{Prob}_M[M([h(\frac{x}{|x|})]) = S(x)] \geq 1 - \varepsilon$ for every string $x \in \Sigma^*$. Without loss of generality, we hereafter assume that $\varepsilon > 0$.

Recall that the notation Σ_Γ denotes an alphabet $\{[\tau] \mid \sigma \in \Sigma, \tau \in \Gamma\}$, and we set $e = |\Sigma_\Gamma|$. For simplicity, write ψ_0 for the triplet $(|q_0\rangle, 0, 0)$ in the space $\mathcal{S} = \text{span}\{E_Q\} \times \mathbb{R} \times \mathbb{R}$. For each element $(x, n) \in \Delta$ and a string $w = \text{Pref}_{|x|}(h(n))$, $\hat{T}_{\dagger[w]} \psi_0$ is assumed to have the form $(|\phi_x\rangle, \gamma_{x,1}, \gamma_{x,2})$.

As the first step, we want to define a relation \equiv_S to satisfy Condition 5. For time being, however, we define \equiv_S as a subset of $\bigcup_{n \in \mathbb{N}} (\Delta_n \times \Delta_n)$, where Δ_n denotes the set $\{(x, n) \mid |x| \leq n\}$; later, we will expand it to $\Delta \times \Delta$, as required by the lemma. Given a pair $(x, n), (y, n) \in \Delta_n$, let $(x, n) \equiv_S (y, n)$ whenever $S(xz) = S(yz)$ for all strings z satisfying $|xz| = n$. From this definition, it is not difficult to show that \equiv_S satisfies the properties of reflexivity, symmetry, and transitivity; thus, \equiv_S is indeed an equivalence relation.

As the second step, we will define a closeness relation \cong on Δ . For our purpose, we choose a constant μ satisfying $0 < \mu < (1 - 2\varepsilon)/7$. Given two elements $(x, n), (y, m) \in \Delta$, we write $(x, n) \cong (y, m)$ whenever $\left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 < \mu$, where $w = \text{Pref}_{|x|}(h(n))$ and $w' = \text{Pref}_{|y|}(h(m))$. To see Condition 7, let us consider an arbitrary \cong -discrepancy subset G of Δ . In G , any distinct pair $(x, n), (y, m) \in G$ satisfies that $\mu \leq \left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 \leq \sqrt{3}$. Since μ is a positive constant, it is obvious that G is a finite set and thus its cardinality $|G|$ is upper-bounded by an appropriate constant. By setting $d = \max_G \{|G|\}$ over all possible \cong -discrepancy subsets G of Δ , Condition 7 is immediately met.

To show Condition 2, we first claim the following statement.

Claim 1 *For any two elements $(x, n), (y, n) \in \Delta$ with $|x| = |y|$, if $\left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 < 1 - 2\varepsilon$, then $(x, n) \equiv_S (y, n)$ holds.*

Condition 2 follows directly from Claim 1 because $(x, n) \cong (y, n)$ implies $\left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 < \mu < 1 - 2\varepsilon$. In order to prove Claim 1, we need to prove two key claims, Claims 2 and 3.

Claim 2 *For any two elements $(x, n), (y, n) \in \Delta$ and any string $z \in \Sigma^*$ with $|x| = |y|$ and $|xz| = n$, it holds that $2 \left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 \geq |p_{acc}(xz) - p_{acc}(yz)| + |p_{rej}(xz) - p_{rej}(yz)|$.*

Proof. By a direct calculation of the norm, we obtain

$$\begin{aligned} \left\| \hat{T}_{\dagger[h(n)]} \psi_0 - \hat{T}_{\dagger[h(n)]} \psi_0 \right\|^2 &= \|(|\phi_{xz}\rangle, p_{acc}(xz), p_{rej}(xz)) - (|\phi_{yz}\rangle, p_{acc}(yz), p_{rej}(yz))\|^2 \\ &= \| |\phi_{xz}\rangle - |\phi_{yz}\rangle \|^2 + |p_{acc}(xz) - p_{acc}(yz)| + |p_{rej}(xz) - p_{rej}(yz)| \\ &\geq |p_{acc}(xz) - p_{acc}(yz)| + |p_{rej}(xz) - p_{rej}(yz)|. \end{aligned}$$

On the contrary, since $\hat{T}_{\dagger[wu]} \psi_0 = \hat{T}_{\dagger[w]} \left(\hat{T}_{\dagger[u]} \psi_0 \right)$ and $\hat{T}_{\dagger[w'u]} \psi_0 = \hat{T}_{\dagger[w']} \left(\hat{T}_{\dagger[u]} \psi_0 \right)$, Lemma 3.1(3) leads to the following inequality:

$$\left\| \hat{T}_{\dagger[h(n)]} \psi_0 - \hat{T}_{\dagger[h(n)]} \psi_0 \right\|^2 \leq 2 \left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2.$$

By combining the above two inequalities, it immediately follows that $2 \left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 \geq |p_{acc}(xz) - p_{acc}(yz)| + |p_{rej}(xz) - p_{rej}(yz)|$, as requested. \square

Claim 3 *If $|x| = |y| \leq n$ and $\left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 < 1 - 2\varepsilon$, then $S(xz) = S(yz)$ holds for all strings $z \in \Sigma^*$ satisfying $|xz| = n$.*

Proof. To lead to a contradiction, we assume that $\left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 < 1 - 2\varepsilon$ and that an appropriately chosen string z satisfies both $|xz| = n$ and $S(xz) \neq S(yz)$. This second assumption (concerning z) implies that either (i) $p_{acc}(xz) \geq 1 - \varepsilon$ and $p_{rej}(yz) \geq 1 - \varepsilon$, or (ii) $p_{rej}(xz) \geq 1 - \varepsilon$ and $p_{acc}(yz) \geq 1 - \varepsilon$. In either case, we conclude that $|p_{acc}(xz) - p_{acc}(yz)| \geq 1 - 2\varepsilon$ and $|p_{rej}(xz) - p_{rej}(yz)| \geq 1 - 2\varepsilon$. By appealing to Claim 2, we obtain

$$2 \left\| \hat{T}_{\dagger[w]} \psi_0 - \hat{T}_{\dagger[w']} \psi_0 \right\|^2 \geq |p_{acc}(xz) - p_{acc}(yz)| + |p_{rej}(xz) - p_{rej}(yz)| \geq 2(1 - 2\varepsilon).$$

This contradicts our first assumption that $\left\| \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0 - \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0 \right\|^2 < 1 - 2\varepsilon$. Therefore, the equation $S(xz) = S(yz)$ should hold for any string z of length $n - |x|$. \square

Finally, Claim 1 is proven in the following way. Assuming $\left\| \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0 - \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0 \right\|^2 < 1 - 2\varepsilon$, Claim 3 yields the equality $S(xz) = S(yz)$ for any string z of length $n - |x|$. This obviously implies the equivalence $(x, n) \equiv_S (y, n)$ because of the definition of \equiv_S . Thus, Claim 1 should be true.

To show Condition 1, we will first expand a scope of \equiv_S from $\bigcup_{n \in \mathbb{N}} (\Delta_n \times \Delta_n)$ to $\Delta \times \Delta$. Before giving a precise definition of \equiv_S , we quickly discuss an upper-bound of the cardinality $|\Delta_n / \equiv_S|$.

Claim 4 For every length $n \in \mathbb{N}$, $|\Delta_n / \equiv_S| \leq d$ holds.

Proof. Let us assume otherwise. Fix an appropriate number $n \in \mathbb{N}$ and take $d + 1$ different strings $x_1, x_2, \dots, x_{d+1} \in \Sigma^n$ so that $(x_i, n) \not\equiv_S (x_j, n)$ for every distinct pair $i, j \in [d + 1]$. From Condition 2 follows the inequality $(x_i, n) \not\equiv_S (x_j, n)$. Therefore, the set $G = \{(x_i, n) \mid i \in [d + 1]\}$ becomes a \cong -discrepancy subset of Δ_n . Condition 7 then implies $|G| \leq d$. Since this obviously contradicts $|G| = d + 1$, the claim should hold. \square

Since $|\Delta_n / \equiv_S| \leq d$ by Claim 4, the set Δ_n / \equiv_S , for each length $n \in \mathbb{N}$, may be expressed as $\{A_{n,1}, A_{n,2}, \dots, A_{n,d}\}$, provided that, in case of $|\Delta_n / \equiv_S| < d$ for a certain n , we automatically set $A_{n,i} = \emptyset$ for any index i with $|\Delta_n / \equiv_S| < i \leq d$. Now, we will expand \equiv_S in the following natural way. For two arbitrary elements (x, n) and (y, m) in Δ with $n \neq m$, let $(x, n) \equiv_S (y, m)$ if there exists an index $i \in [d]$ such that $(x, n) \in A_{n,i}$ and $(y, m) \in A_{m,i}$. Note that this extended version of \equiv_S is also an equivalence relation. From the above definition of \equiv_S , Δ / \equiv_S is obviously finite, and hence Condition 1 is satisfied.

The desired partial order \leq_S on Δ is defined as follows. Let $(x, n) \leq_S (y, m)$ if there exist two numbers $s, s' \in \mathbb{N}$ for which (i) $0 \leq s \leq s' \leq \lceil 1/\mu \rceil$, (ii) $(s - 1)\mu < \|\phi_x\|^2 \leq s\mu$, and (iii) $(s' - 1)\mu < \|\phi_y\|^2 \leq s'\mu$. As remarked earlier, we write $(x, n) =_S (y, m)$ exactly when $(x, n) \leq_S (y, m)$ and $(y, m) \leq_S (x, n)$. In particular, when $(x, n) =_S (y, m)$ holds, we obtain $|\|\phi_y\|^2 - \|\phi_x\|^2| < \mu$. It is easy to check that \leq_S is reflexive, antisymmetric, and transitive; thus, \leq_S is truly a partial order. Since $\|\phi_{x\sigma}\| \leq \|\phi_x\|$ always holds for any pair $(x, \sigma) \in \Sigma^* \times \Sigma$, we instantly conclude that $(x\sigma, n) \leq_S (x, n)$. Therefore, Condition 3 is met.

Regarding Condition 6, we set the desired constant c to be $\lceil 1/\mu \rceil + 1$. Note that $\|\phi_\lambda\| = 1$ and $\|\phi_x\| \leq \varepsilon$ for all strings x of length n , since either $p_{acc}(x) \geq 1 - \varepsilon$ or $P_{rej}(x) \geq 1 - \varepsilon$ always holds. Consider any strictly descending chain (w.r.t. $<_S$) $(x_e, n_e) <_S (x_{e-1}, n_{e-1}) <_S \dots <_S (x_1, n - 1)$ of length e in Δ . It should hold that $|\|\phi_{x_i}\|^2 - \|\phi_{x_{i+1}}\|^2| \geq \mu$ for any index $i \in [0, e - 1]_{\mathbb{Z}}$. This implies

$$|\|\phi_{x_1}\|^2 - \|\phi_{x_e}\|^2| \geq \sum_{i=1}^{e-1} (|\|\phi_{x_i}\|^2 - \|\phi_{x_{i+1}}\|^2|) \geq (e - 1)\mu.$$

Since $|\|\phi_{x_1}\|^2 - \|\phi_{x_e}\|^2| \leq 1$ holds, $(e - 1)\mu \leq 1$ immediately follows; therefore, we conclude that $e \leq 1 + 1/\mu \leq c$. Condition 6 thus follows.

The remaining condition to verify is Condition 4. To show this condition, we will prove Claim 5, which follows from Lemmas 3.1(1)&(4).

Claim 5 Let $\alpha \in (0, 1]$. Assume that $|x| = |y|$ and $|xz| \leq n$. If $\left\| \hat{T}_{\hat{\mathfrak{f}}[wu]} \psi_0 - \hat{T}_{\hat{\mathfrak{f}}[wu]} \psi_0 \right\|^2 < \gamma$, $\|\phi_x\|^2 - \|\phi_{xz}\|^2 < \alpha$, and $|\|\phi_y\|^2 - \|\phi_{yz}\|^2| < \alpha$, then $\left\| \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0 - \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0 \right\|^2 < \gamma + 9\alpha$, where w and u satisfy $wu = \text{Pref}_{|xz|}(h(n))$ with $|w| = |x|$ and $|u| = |z|$.

Proof of Claim 5. Since $|\phi_{xz}\rangle = T_{\hat{\mathfrak{f}}[u]} |\phi_x\rangle$ and $|\phi_{yz}\rangle = T_{\hat{\mathfrak{f}}[u]} |\phi_y\rangle$, Lemma 3.1(1) implies

$$|\|\phi_x\|^2 - \|\phi_y\|^2 - \|\phi_{xz}\|^2 - \|\phi_{yz}\|^2| \leq 2 [|\|\phi_x\|^2 - \|\phi_{xz}\|^2| + |\|\phi_y\|^2 - \|\phi_{yz}\|^2|] \leq 2\alpha.$$

For convenience, we set $\psi = \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0$ and $\psi' = \hat{T}_{\hat{\mathfrak{f}}[w]} \psi_0$. Those ψ and ψ' satisfy that $\hat{T}_{\hat{\mathfrak{f}}[u]} \psi = \hat{T}_{\hat{\mathfrak{f}}[wu]} \psi_0$ and $\hat{T}_{\hat{\mathfrak{f}}[u]} \psi' = \hat{T}_{\hat{\mathfrak{f}}[wu]} \psi_0$. Furthermore, since $\psi = (|\phi_x\rangle, \gamma_{1,x}, \gamma_{2,x})$ and $\psi' = (|\phi_y\rangle, \gamma_{1,y}, \gamma_{2,y})$ for certain values

$\gamma_{1,x}, \gamma_{2,x}, \gamma_{1,y}, \gamma_{2,y} \in [0, 1]$, we apply Lemma 3.1(4) and then obtain

$$\|\psi - \psi'\|^2 \leq \left\| \hat{T}_{\hat{\mathfrak{f}}[z_u]} \psi - \hat{T}_{\hat{\mathfrak{f}}[z_u]} \psi' \right\|^2 + 3 [\|\phi_x\rangle - \|\phi_y\rangle\|^2 - \|\phi_{xz}\rangle - \|\phi_{yz}\rangle\|^2] < \gamma + 6\alpha.$$

□

To verify Condition 4, let us assume that $(x, n) \cong (y, n)$, $(x\sigma, n) =_S (x, n)$, and $(yz, n) =_S (y, n)$. In other words, $\left\| \hat{T}_{\hat{\mathfrak{f}}[x]} \psi_0 - \hat{T}_{\hat{\mathfrak{f}}[y]} \psi_0 \right\|^2 < \mu$, $\|\phi_{xz}\rangle\|^2 - \|\phi_x\rangle\|^2 < \mu$, and $\|\phi_{yz}\rangle\|^2 - \|\phi_y\rangle\|^2 < \mu$. By setting $\alpha = \gamma = \mu$ in Claim 5, we conclude that $\left\| \hat{T}_{\hat{\mathfrak{f}}[x]} \psi_0 - \hat{T}_{\hat{\mathfrak{f}}[y]} \psi_0 \right\|^2 < 7\mu$. Since $7\mu < 1 - 2\varepsilon$, Claim 1 yields the equivalence $(x, n) \equiv_S (y, n)$, as requested.

The proof of Theorem 3.4 is now completed. □

Theorem 3.4 reveals a certain aspect of the characteristic features of advised 1qfa's, from which we can deduce several important consequences. Here, we will apply Theorem 3.4 to show a class separation between REG and 1QFA/ n . Without use of advice, Kondacs and Watrous [7] already proved that $\text{REG} \not\subseteq \text{1QFA}$. Our class separation between REG and 1QFA/ n indicates that 1qfa's are still not as powerful as 1dfa's even with a great help of advice.

Corollary 3.5 $\text{REG} \not\subseteq \text{1QFA}/n$, and thus $\text{1QFA}/n \neq \text{REG}/n$.

Proof. Our example language S over an alphabet $\Sigma = \{a, b\}$ is expressed in a form of regular expression as $(aa + ab + ba)^*$. Since S is obviously a regular language, hereafter we intend to show that S is not in 1QFA/ n . Assume otherwise; that is, S belongs to 1QFA/ n . Letting $\Delta = \{(x, n) \in \Sigma^* \times \mathbb{N} \mid |x| \leq n\}$, Theorem 3.4 guarantees the existence of two constants $c, d \in \mathbb{N}^+$, an equivalence relation \equiv_S , a partial order \leq_S , and a closeness relation \cong that satisfy Conditions 1–7 given in the theorem. Let e be the total number of equivalence classes in Δ / \equiv_S and set $k = \max\{c, d, e\}$. Moreover, let n denote the minimal *even* integer satisfying $n \geq (2k + 1)(\lceil \log k \rceil + 1)$.

To draw a contradiction, we want to construct a special string x of length at most n . Inductively, we build a series of strings x_1, x_2, \dots, x_m , where each x_i has length at most $2(\lceil \log k \rceil + 1)$, so that they maximize the total length $|x_1 \cdots x_m|$ that does not exceed n . For our convenience, set $x_0 = \lambda$. The construction of such a series is described as follows. Assuming that $x_0, x_1, x_2, \dots, x_i$ are already defined, we want to define x_{i+1} in the following way. Let us denote by \bar{x}_i the concatenated string $x_1 x_2 \cdots x_i$ and denote by $z_{i,w}$ the string $\bar{x}_i w$ for any given string w in $((a + b)a)^*$ satisfying the inequity $|\bar{x}_i w| \leq n$. Now, we claim our key statement.

Claim 6 *There exists a nonempty string w in $((a + b)a)^*$ such that $|w| \leq 2(\lceil \log k \rceil + 1)$ and $(z_{i,w}, n) <_S (\bar{x}_i, n)$.*

Assuming that Claim 6 is true, we choose the lexicographically-first nonempty string w in $((a + b)a)^*$ that satisfies both $|w| \leq 2(\lceil \log k \rceil + 1)$ and $(z_{i,w}, n) <_S (\bar{x}_i, n)$. The desired string x_{i+1} in our construction is defined to be this special string w . Hence, $\bar{x}_{i+1} = \bar{x}_i x_{i+1}$ holds. After the whole construction, it holds that $|x_1 x_2 \cdots x_m| \leq 2m(\lceil \log k \rceil + 1)$. Our construction ensures that $(\bar{x}_m, n) <_S (\bar{x}_{m-1}, n) <_S \cdots <_S (\bar{x}_1, n)$; thus, the sequence $((\bar{x}_m, n), (\bar{x}_{m-1}, n), \dots, (\bar{x}_1, n))$ forms a strictly descending chain in Δ . Since $m \leq c$ by Condition 6, $m \leq k$ follows. We therefore conclude that $|x_1 x_2 \cdots x_m| > n - 2(\lceil \log k \rceil + 1)$ because, otherwise, there still remains enough room for another string x_{m+1} to satisfy, by Claim 6, that $|x_{m+1}| \leq 2(\lceil \log k \rceil + 1)$ and $(\bar{x}_{m+1}, n) <_S (\bar{x}_m, n)$, contradicting the maximality of the length $|x_1 x_2 \cdots x_m|$. As a result, we obtain $n - 2(\lceil \log k \rceil + 1) < |x_1 x_2 \cdots x_m| \leq 2k(\lceil \log k \rceil + 1)$, from which we conclude that $n < (2k + 1)(\lceil \log k \rceil + 1)$. This is clearly a contradiction since $n \geq (2k + 1)(\lceil \log k \rceil + 1)$. Therefore, S cannot belong to 1QFA/ n .

To complete the proof of the proposition, it still remains to prove Claim 6. This claim can be proven by a way of contradiction with a careful use of Conditions 4, 5, and 7. Let us assume that \bar{x}_i is already defined. Toward a contradiction, we suppose that the claim fails; that is, for any nonempty string $w \in ((a + b)a)^*$ with $|w| \leq 2(\lceil \log k \rceil + 1)$, the equality $(z_{i,w}, n) =_S (\bar{x}_i, n)$ holds. Under this assumption, it is possible to prove the following statement.

Claim 7 *For any two distinct pair w, w' in S with $|w| = |w'| \leq n - 2$, it holds that $(wa, n) \not\equiv_S (w'b, n)$.*

Let X_k denote the set of all strings in $((a + b)a)^*$ of length exactly $2(\lceil \log k \rceil + 1)$. Assuming that Claim 7 is true, let us consider those strings in X_k . Note that the total number of such strings is $2^{\lceil \log k \rceil + 1} \geq 2k$.

We define G_n to be the set of all elements $(z_{i,w}, n) \in \Delta$ associated with certain strings w in X_k . Note that $|G_n| = |X_k| \geq 2k$. Now, we want to show that G_n is a \cong -discrepancy set. Assume otherwise; that is, two *distinct* strings $w, w' \in X_k$ satisfy $(z_{i,w}, n) \cong (z_{i,w'}, n)$. For those strings, there are (possibly empty) strings y, y', z for which $w = yaaz$ and $w' = y'baz$. Note that $|\bar{x}_i y| = |\bar{x}_i y'| - 2 \leq |z_{i,w}| \leq n - 2$ since $|z_{i,w}| \leq n$. By applying Claim 7 to the two strings $\bar{x}_i y$ and $\bar{x}_i y'$, we conclude that $(\bar{x}_i ya, n) \not\equiv_S (\bar{x}_i y' b, n)$. Since $(z_{i,w}, n) =_S (\bar{x}_i, n) =_S (z_{i,w'}, n)$ by our assumption, Condition 4 then implies that $(\bar{x}_i ya, n) \equiv_S (\bar{x}_i y' b, n)$. This is a contradiction, and therefore G_n is indeed a \cong -discrepancy subset of Δ . Condition 7 implies that $|G_n| \leq d \leq k$. However, this contradicts $|G_n| \geq 2k$. Therefore, Claim 6 should hold.

Finally, let us prove Claim 7 by induction on length $|w|$. Consider the case where $|w| = 0$. Assume that $(a, n) \equiv_S (b, n)$. The definition of S implies the existence of a string z for which $|az| = n$ and $S(az) \neq S(bz)$. For instance, when $n = 2$, it holds that $S(ab) \neq S(bb)$. However, Condition 5 yields $S(az) = S(bz)$, leading to a contradiction. Thus, it follows that $(a, n) \not\equiv_S (b, n)$. Next, consider the case where $0 < |w| \leq n - 2$. Since $w, w' \in S$, there exists a string z such that $|wabz| = n$ and $S(wabz) \neq S(w'bbz)$. If $(wa, n) \equiv_S (w'b, n)$, then Condition 5 implies $S(wabz) = S(w'bbz)$, a contradiction. We thus conclude that $(wa, n) \not\equiv_S (w'b, n)$. \square

4 Power of Reversible Computation with Advice

As a special case of quantum computation, we turn our attention to error-free quantum computation and we wish to discuss characteristic behaviors of such computation, particularly assisted by useful deterministic advice. Since error-free quantum computation has been known to coincide with “reversible” computation, we are focused on a model of *one-way (deterministic) reversible finite automaton* (or 1rfa, in short). In this paper, a 1rfa is introduced as a 1dfa $M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ that satisfies a particular condition, called a “reversibility condition”; namely, for every inner state $q \in Q$ and every symbol $\sigma \in \tilde{\Sigma}$, there exists at most one inner state $q' \in Q$ that makes a transition $\delta(q', \sigma) = q$. We use the notation 1RFA for the family of all languages recognized by 1rfa’s. Analogous to REG/ n , the advised language family 1RFA/ n is composed of all languages L over appropriate alphabets Σ such that there exist a 1rfa M and an advice function h satisfying (i) $|h(n)| = n$ for any length $n \in \mathbb{N}$ and (ii) $M([h(\frac{x}{|x|})]) = L(x)$ for every string $x \in \Sigma^*$. From the obvious relation $1RFA \subseteq 1QFA$ follows the containment $1RFA/n \subseteq 1QFA/n$.

In Theorem 3.4, we have presented a machine-independent, algebraic sufficient condition for languages recognized by advised 1qfa’s. When underlying finite automata are restricted on 1rfa’s, it is possible to strengthen the theorem with a precise machine-independent, algebraic characterization of languages by advised 1rfa’s. Here, we will describe the second main theorem, Theorem 4.1.

Theorem 4.1 *Let S be any language over alphabet Σ and set $\Delta = \{(x, n) \mid x \in \Sigma^*, n \in \mathbb{N}, |x| \leq n\}$. The following two statements are logically equivalent.*

1. S is in 1RFA/ n .
2. There is an equivalence relation \equiv_S over Δ such that
 - (i) the set Δ/\equiv_S is finite, and
 - (ii) for any length parameter $n \in \mathbb{N}$, any symbol $\sigma \in \Sigma$, and any two elements $(x, n), (y, n) \in \Delta$ with $|x| = |y|$, the following two conditions hold.
 - (a) Whenever $|x\sigma| \leq n$, $(x\sigma, n) \equiv_S (y\sigma, n)$ iff $(x, n) \equiv_S (y, n)$.
 - (b) If $(x, n) \equiv_S (y, n)$, then $S(xz) = S(yz)$ holds for all strings $z \in \Sigma^*$ satisfying $|xz| = n$.

This theorem requires only one equivalence relation \equiv_S , compared to Theorem 3.4. Condition (a) in this theorem particularly concerns the *reversibility* of underlying automata. Hereafter, we intend to give the proof of Theorem 4.1.

Proof of Theorem 4.1. Let Σ be any alphabet, set $\Delta = \{(x, n) \mid x \in \Sigma^*, n \in \mathbb{N}, |x| \leq n\}$, and consider an arbitrary language S over Σ .

(1 \Rightarrow 2) Assuming $S \in 1RFA/n$, we take an advice alphabet Γ , a 1rfa $M = (Q, \Sigma_\Gamma, \delta, q_0, Q_{acc}, Q_{rej})$, and an advice function $h : \mathbb{N} \rightarrow \Gamma^*$ satisfying $M([h(\frac{x}{|x|})]) = S(x)$ for all strings $x \in \Sigma^*$. Now, we give the desired relation \equiv_S on Δ by defining $(x, n) \equiv_S (y, m)$ exactly when there exists an inner state $q \in Q$ for which M enters q just after reading $[\frac{x}{w}]$ as well as after reading $[\frac{y}{w'}]$, where w and w' are strings specified by

$w = \text{Pref}_{|x|}(h(n))$ and $w' = \text{Pref}_{|y|}(h(m))$. Clearly, the relation \equiv_S is reflexive, symmetric, and transitive; thus, it is an equivalence relation. The next goal is to establish Conditions (i)–(ii).

(i) Since Q is finite, there are only a finite number of equivalence classes in the set Δ/\equiv_S .

(ii) Take any symbol $\sigma \in \Sigma$ and two arbitrary elements $(x, n), (y, n)$ in Δ satisfying $|x| = |y|$.

(a) Assume that $|x\sigma| \leq n$. Using the aforementioned string w , let τ denote an advice symbol satisfying $w\tau = \text{Pref}_{|x\sigma|}(h(n))$. If $(x\sigma, n) \equiv_S (y\sigma, n)$ holds, then M must enter the same inner state in Q after reading $\begin{bmatrix} x\sigma \\ w\tau \end{bmatrix}$ as well as after reading $\begin{bmatrix} y\sigma \\ w\tau \end{bmatrix}$. Since M is reversible, it should enter a unique inner state, say, p after reading $\begin{bmatrix} x \\ w \end{bmatrix}$ as well as after reading $\begin{bmatrix} y \\ w \end{bmatrix}$. This leads to a conclusion $(x, n) \equiv_S (y, n)$. Similarly, we can show that $(x, n) \equiv_S (y, n)$ implies $(x\sigma, n) \equiv_S (y\sigma, n)$. Therefore, Condition (a) in the theorem is satisfied.

(b) Let z be any string satisfying $|xz| = n$. Assume that $(x, n) \equiv_S (y, n)$ holds. This means that M enters the same inner state after reading $\begin{bmatrix} x \\ w \end{bmatrix}$ as well as after reading $\begin{bmatrix} y \\ w \end{bmatrix}$. Since M is deterministic, M must behave exactly in the same way on the remaining input string $\begin{bmatrix} z \\ u \end{bmatrix}$, where u satisfies $wu = \text{Pref}_n(h(n))$. Therefore, M accepts $\begin{bmatrix} xz \\ wu \end{bmatrix}$ iff M accepts $\begin{bmatrix} yz \\ wu \end{bmatrix}$. In other words, $S(xz) = S(yz)$ holds, as requested.

(2 \Rightarrow 1) To make our proof simple, we ignore the empty string and consider only the set $S \cap \Sigma^+$. Assume that we have an equivalence relation \equiv_S that satisfies Conditions (i)–(ii) of the theorem. In what follows, we will show that S is indeed in 1RFA/ n . By Condition (i), we set $d = |\Delta/\equiv_S|$ and assume that $\Delta/\equiv_S = \{A_1, A_2, \dots, A_d\}$, where each A_i is an equivalence class.

Given any length $n \in \mathbb{N}^+$, we set $C_{acc}^{(n)} = \{q \in [d] \mid \exists x_0 \in \Sigma^n [(x_0, n) \in A_q \wedge S(x_0) = 1]\}$ and $C_{rej}^{(n)} = \{q \in [d] \mid \exists x_0 \in \Sigma^n [(x_0, n) \in A_q \wedge S(x_0) = 0]\}$. Obviously, two sets $\{C_{acc}^{(n)} \mid n \in \mathbb{N}^+\}$ and $\{C_{rej}^{(n)} \mid n \in \mathbb{N}^+\}$ are both finite.

Claim 8 For any $n \in \mathbb{N}^+$, $x, y \in \Sigma^*$, and $\sigma \in \Sigma$, the following four properties hold.

1. For any element $(x, n) \in \Delta$, there is a unique index $q \in [d]$ such that $(x, n) \in A_q$.
2. If $(x, n), (y, n) \in A_q$ with $q \in [d]$ and $|x| = |y| < n$, then there exists a unique index $q' \in [d]$ such that $(x\sigma, n), (y\sigma, n) \in A_{q'}$.
3. If $(x\sigma, n), (y\sigma, n) \in A_{q'}$ with $q' \in [d]$, then there exists a unique index $q \in [d]$ for which $(x, n), (y, n) \in A_q$.
4. It holds that $C_{acc}^{(n)} \cap C_{rej}^{(n)} = \emptyset$ and that $\{(x, n) \in \Delta \mid x \in S \cap \Sigma^n\} \subseteq \bigcup_{q \in C_{acc}^{(n)}} A_q$ and $\{(x, n) \in \Delta \mid x \in \Sigma^n - S\} \subseteq \bigcup_{q \in C_{rej}^{(n)}} A_q$.

Proof. (1) Since the set $\bigcup_{i=1}^d A_i$ covers Δ , each element (x, n) in Δ belongs to a certain set, say, A_{i_0} . The uniqueness of this index i_0 comes from the fact that all sets in Δ/\equiv_S are mutually disjoint.

(2) Since A_q is an equivalence class, $(x, n), (y, n) \in A_q$ implies $(x, n) \equiv_S (y, n)$. Moreover, since $|x\sigma| \leq n$, $(x\sigma, n) \equiv_S (y\sigma, n)$ immediately follows from $(x, n) \equiv_S (y, n)$ by Condition (a). We then apply (1) to obtain a unique index $q' \in [d]$ for which $(x\sigma, n), (y\sigma, n) \in A_{q'}$ holds.

(3) We obtain $(x\sigma, n) \equiv_S (y\sigma, n)$ from $(x\sigma, n), (y\sigma, n) \in A_{q'}$. Condition (a) then ensures that $(x, n) \equiv_S (y, n)$. The desired consequence follows from (1).

(4) Assume that $|x| = |y| = n$. The containment $\{(x, n) \in \Delta \mid x \in S \cap \Sigma^n\} \subseteq \bigcup_{q \in C_{acc}^{(n)}} A_q$ is obvious from the definition of $C_{acc}^{(n)}$. Similarly, the other containment regarding $C_{rej}^{(n)}$ also holds. Finally, we will show the disjointness of $C_{acc}^{(n)}$ and $C_{rej}^{(n)}$. Assuming that a certain inner state q exists inside $C_{acc}^{(n)} \cap C_{rej}^{(n)}$, we take two elements $(x, n), (y, n) \in A_q$ satisfying $S(x) \neq S(y)$. On the contrary, using Condition (b), from $(x, n), (y, n) \in A_q$ (thus, $(x, n) \equiv_S (y, n)$) follows the equality $S(x) = S(y)$. This is a contradiction, and hence $C_{acc}^{(n)} \cap C_{rej}^{(n)}$ should be empty. \square

Based on Claim 8, we wish to define an appropriate advice function h . For this purpose, let $n \in \mathbb{N}^+$ be an arbitrary length and let $\#$ be a special symbol. Given every index $i \in [n]$, we will introduce *finite* functions $h_{n,i} : [d] \times \Sigma \rightarrow [d] \cup \{\#\} \cup ([d] \times \{C_{acc}^{(n)}\}_{n \in \mathbb{N}^+} \times \{C_{rej}^{(n)}\}_{n \in \mathbb{N}^+})$. Let q and q' be any two indices in $[d]$ and let σ be any symbol in Σ .

- (i) Let $h_{1,1}(q, \sigma) = (q', C_{acc}^{(1)}, C_{rej}^{(1)})$ if $(\sigma, 1) \in A_{q'}$ holds.
- (ii) For $n \geq 2$, let $h_{n,1}(q, \sigma) = q'$ if $(\sigma, n) \in A_{q'}$ holds.
- (iii) When $i \in [2, n-1]$, let $h_{n,i}(q, \sigma) = q'$ if both $(x, n) \in A_q$ and $(x\sigma, n) \in A_{q'}$ hold for an appropriate string $x \in \Sigma^{i-1}$.
- (vi) Let $h_{n,n}(q, \sigma) = (q', C_{acc}^{(n)}, C_{rej}^{(n)})$ if both $(x, n) \in A_q$ and $(x\sigma, n) \in A_{q'}$ hold for an appropriate string $x \in \Sigma^{n-1}$.

- (v) In the above definitions, to make $h_{n,i}$ a total function, whenever no string $x \in \Sigma^{i-1}$ satisfies $(x, n) \notin A_q$, we set $h_{n,i}(q, \sigma) = \#$ for any symbol $\sigma \in \Sigma$.

We set $\Gamma = \{h_{n,i} \mid n \geq 1, i \in [n]\}$. Since Γ is a finite set, we enumerate all the functions in Γ as h'_1, h'_2, \dots, h'_e and we treat each function h'_i as a new “advice symbol.” Our advice string $h(n)$ of length n is set to be $h_{n,1}h_{n,2} \cdots h_{n,n}$, where each $h_{n,i}$ corresponds to a unique advice symbol listed above.

Claim 9 *The above defined h is indeed a function.*

Proof. For every symbol $\sigma \in \Sigma$, Claim 8(1) provides a unique inner state $q' \in Q$ that satisfies $(\sigma, n) \in A_{q'}$. This proves that $h_{n,1}$ is a function. Next, let $i \in [2, n-1]_{\mathbb{Z}}$ and assume that $h_{n,i}(q, \sigma) = q'$ and $h_{n,i}(q, \sigma) = q''$. By the definition of $h_{n,i}$, we can take two strings $x, y \in \Sigma^{i-1}$ such that $(x, n), (y, n) \in A_q$, $(x\sigma, n) \in A_{q'}$, and $(y\sigma, n) \in A_{q''}$. Since $|x| = |y| < n$, Claim 8(2) implies $q' = q''$. The case where $i = n$ is similarly proven by Claim 8(2). \square

Next, we will define a finite automaton $M = (Q, \Sigma_{\Gamma}, \delta, q_0, Q_{acc}, Q_{rej})$ with $q_0 = 0$. The set Q_{acc} (resp., Q_{rej}) consists of all pairs of the form $(q, C_{acc}^{(n)}, C_{rej}^{(n)})$ for any length $n \in \mathbb{N}^+$ and any $q \in C_{acc}^{(n)}$ (resp., $q \in C_{rej}^{(n)}$). Finally, using the notation $Q_{halt} (= Q_{acc} \cup Q_{rej})$, we define $Q = Q_{halt} \cup \{q_0\} \cup [d]$. Recall that $\Sigma_{\Gamma} = \{[\frac{\sigma}{\tau}] \mid \sigma \in \Sigma, \tau \in \Gamma\}$. Our transition function δ is defined as follows. Let $n \in \mathbb{N}^+$. Initially, we set $\delta(q_0, \phi) = q_0$ and $\delta(q, \$) = q$ for every inner state q in Q_{halt} . If $h_{n,1}(1, \sigma) \neq \#$, then we define $\delta(q_0, [\frac{\sigma}{h_{n,1}}]) = h_{n,1}(1, \sigma)$. Given an index $i \in [2, n]_{\mathbb{Z}}$ and an inner state $q \in [d]$, if $h_{n,i}(q, \sigma) \neq \#$, then we set $\delta(q, [\frac{\sigma}{h_{n,i}}]) = h_{n,i}(q, \sigma)$. For convenience, we say that all input pairs $(q, [\frac{\sigma}{\tau}])$ defined so far are *legitimate* for δ . With the correct advice function h , the automaton M on input $[\frac{x}{h(x)}]$ never reaches any other remaining input pairs $(q, [\frac{\sigma}{\tau}])$, which are distinctively called *illegitimate*. We may define the values of $\delta(q, [\frac{\sigma}{\tau}])$ arbitrarily so that δ is “reversible” on the set of all illegitimate input pairs.

Claim 10 *The machine M is a 1rfa.*

Proof. Using Claim 8, we want to prove by induction on i (for $h_{n,i}$) that M is “reversible” on the set of all legitimate input pairs given to δ . To achieve this goal, we need to verify the reversibility condition of δ ; that is, for every $\sigma \in \Sigma$, $q' \in Q$, and $i \in [n]$, if $(q, [\frac{\sigma}{\tau}])$ is a legitimate pair, then there is at most one inner state $q \in Q$ such that $\delta(q, [\frac{\sigma}{h_{n,i}}]) = q'$. To show this, assume that $\delta(q_1, [\frac{\sigma}{h_{n,i}}]) = q'$ and $\delta(q_2, [\frac{\sigma}{h_{n,i}}]) = q'$.

[Case: $n = i = 1$] Our assumption implies that q' has the form $(q'', C_{acc}^{(1)}, C_{rej}^{(1)})$ for a certain index $q'' \in [d]$. The legitimacy of input pairs $(q_1, [\frac{\sigma}{h_{1,1}}])$ and $(q_2, [\frac{\sigma}{h_{1,1}}])$ instantly yields the equality $q_1 = q_2$.

[Case: $n \geq 2$ and $i = 1$] Consider the case where $q' = h_{n,1}(1, \sigma)$. In terms of “legitimacy,” we have demanded that no inner state q other than q_0 satisfies $\delta(q, [\frac{\sigma}{h_{n,1}}]) = q'$; thus, we obtain $q_1 = q_2 = q_0$.

[Case: $1 < i < n$] By the assumption, it follows that $q' = h_{n,i}(q_1, \sigma) = h_{n,i}(q_2, \sigma)$. Since $q' \neq \#$, we take two strings $x, y \in \Sigma^{i-1}$ such that $(x, n) \in A_{q_1}$, $(y, n) \in A_{q_2}$, and $(x\sigma, n), (y\sigma, n) \in A_{q'}$. By Claim 8(3), the equality $q_1 = q_2$ follows immediately.

[Case: $i = n \geq 2$] Since $q' = h_{n,n}(q_1, \sigma) = h_{n,n}(q_2, \sigma) = (q'', C_{acc}^{(n)}, C_{rej}^{(n)})$, there are two strings $x, y \in \Sigma^{n-1}$ for which $(x, n) \in A_{q_1}$, $(y, n) \in A_{q_2}$, and $(x\sigma, n), (y\sigma, n) \in A_{q''}$. Claim 8(3) then implies $q_1 = q_2$, as requested. \square

Finally, we want to show that $S = \{x \mid M \text{ accepts } [\frac{x}{h(x)}]\}$. Fix $n \in \mathbb{N}$ and assume that $x = \sigma_1\sigma_2 \cdots \sigma_n \in \Sigma^n$ and $(\lambda, n) \in A_{q_0}$, $(\sigma_1, n) \in A_{q_1}$, $(\sigma_1\sigma_2, n) \in A_{q_2}$, \dots , $(x, n) \in A_{q_n}$. First, we consider the case where $x \in S$. We will prove by induction on $i \in [0, n]_{\mathbb{Z}}$ that $q_i = \hat{\delta}(q_0, [\frac{\sigma_1 \cdots \sigma_i}{h_{n,1} \cdots h_{n,i}}])$, where $\hat{\delta}$ is the *extended transition function* induced from δ . From the induction hypothesis on i , it immediately follows that

$$\hat{\delta}(q_0, [\frac{\sigma_1 \cdots \sigma_{i+1}}{h_{n,1} \cdots h_{n,i+1}}]) = h_{n,i+1}(\hat{\delta}(q_0, [\frac{\sigma_1 \cdots \sigma_i}{h_{n,1} \cdots h_{n,i}}]), \sigma_{i+1}) = h_{n,i+1}(q_i, \sigma_{i+1}) = q_{i+1}.$$

Since $x \in S$, by Claim 8(3), q_n must have the form $(q, C_{acc}^{(n)}, C_{rej}^{(n)})$ for a certain $q \in C_{acc}^{(n)}$. It thus follows that $\hat{\delta}(q_0, [\frac{x}{h(x)}]) = (q, C_{acc}^{(n)}, C_{rej}^{(n)})$. Since $\hat{\delta}(q_0, [\frac{x}{h(x)}])\$) = \hat{\delta}(q_0, [\frac{x}{h(x)}])$, M accepts $[\frac{x}{h(x)}]$. The other case $x \notin S$ is similarly handled to the previous case, since the essential difference is only the final step.

This completes the proof of Theorem 4.1. \square

As an immediate consequence of Theorem 4.1, we will show that 1QFA is not included in 1RFA/ n . This result can be viewed as a strength of bounded-error quantum computation over error-free advised quantum computation.

Corollary 4.2 $1QFA \not\subseteq 1RFA/n$, and thus $1RFA/n \neq 1QFA/n$.

Proof. Let us consider the language $L = \{0^m 1^n \mid m, n \in \mathbb{N}\}$. Ambainis and Freivalds [2] showed how to recognize this language L on a certain 1qfa with success probability at least 0.68. To obtain the desired consequence, we will show that $L \notin 1RFA/n$. Since L was already shown to be located outside of 1RFA [2], our result therefore extends the result of Ambainis and Freivalds.

To lead to a contradiction, we assume that L belongs to $1RFA/n$. Theorem 4.1 guarantees the existence of an equivalence relation \equiv_L on Δ that satisfies Conditions 1–2 of the theorem. We denote by k the cardinality of the set Δ/\equiv_L of equivalence classes. Let us fix a number n to satisfy $n > k + 1$, and consider a subset of L , $L_n = \{0^i 1^{n-i} \mid i \in [n-1]\}$. Since $|L_n| = n - 1 > k$, there are at least two indices $i, j \in [n-1]$ with $i < j$ for which $(0^i 1^{n-i}, n) \equiv_L (0^j 1^{n-j}, n)$ holds. Applying Condition (a) of the theorem repeatedly (by setting 1), it follows that $(0^i 1^{j-i}, n) \equiv_L (0^j, n)$. If we choose $z = 0^{n-j}$ in Condition (b), then the condition implies $L(0^i 1^{j-i} z) = L(0^j z)$. Since $i < j < n$, however, it holds that $L(0^i 1^{j-i} z) = L(0^i 1^{j-i} 0^{n-j}) = 0$ and that $L(0^j z) = L(0^n) = 1$. This is a contradiction. Therefore, L cannot belong to $1RFA/n$.

To see the second part of the corollary, since $1QFA \subseteq 1QFA/n$, the equality $1RFA/n = 1QFA/n$ leads to the containment $1QFA \subseteq 1RFA/n$. Clearly, this contradicts the first part. Therefore, we conclude that $1RFA/n \neq 1QFA/n$. \square

As a probabilistic variant of deterministic advice, *randomized advice* has been observed to endow an enormous computational power to one-way finite automata, where randomized advice refers to a *probability ensemble* $\{D_n\}_{n \in \mathbb{N}}$ consisting of an infinite series of probability distributions D_n over the set Γ^n of advice strings. Those randomly chosen advice strings are given on the loqwe track of an input tape so that a tape head can scan a standard input and advice simultaneously.

Let us give a quick remark on a power of randomized advice. The notation $1\text{-BPLIN}/Rlin$ denotes the family of all languages recognized with bounded-error probability by one-tape one-head two-way off-line probabilistic Turing machines whose computation paths *all* terminate within *linear time* in the presence of randomized advice of *linear size*. When probabilistic Turing machine is replaced by 1dfa and 1npda, we obtain language families REG/Rn and CFL/Rn , respectively, from $1\text{-BPLIN}/Rlin$. It was shown in [15] that REG/Rn is powerful enough to coincide with $1\text{-BPLIN}/Rlin$. Moreover, it was proven that $REG/Rn \not\subseteq CFL/n$ [15], and thus $CFL/n \neq CFL/Rn$.

Like the notations REG/Rn and CFL/Rn introduced in [15], $1RFA/Rn$ expresses the family of all languages L that satisfy the following condition: there exist a 1rfa M , an error bound $\varepsilon \in [0, 1/2)$, an advice alphabet Γ , and an advice probability ensemble $\{D_n\}_{n \in \mathbb{N}}$ ($D_n : \Gamma^n \rightarrow [0, 1]$) such that, for every length $n \in \mathbb{N}$ and any string $x \in \Sigma^n$, (*) M on input $\begin{bmatrix} x \\ y \end{bmatrix}$ outputs $L(x)$ with probability at least $1 - \varepsilon$ when y is chosen at random according to D_n (i.e., y is chosen with probability $D_n(y)$). For notational convenience, we introduce a succinct notation $\begin{bmatrix} x \\ D_n \end{bmatrix}$ to denote a *random variable* expressing a string $\begin{bmatrix} x \\ y \end{bmatrix}$, provided that $y \in \Gamma^n$ is chosen with probability $D_n(y)$. With this notation, we rephrase Condition (*) as $\text{Prob}_{D_n}[M(\begin{bmatrix} x \\ D_n \end{bmatrix}) = L(x)] \geq 1 - \varepsilon$.

In what follows, we will demonstrate a strength of 1rfa's when they take randomized advice.

Proposition 4.3 1. $DCFL \cap 1RFA/Rn \not\subseteq REG/n$.

2. $1RFA/Rn \not\subseteq CFL/n$.

Proof. (1) For our purpose, we use a “marked” version of Pal , the set of *even-length palindromes*. Now, define $Pal_{\#} = \{w\#w^R \mid w \in \{0, 1\}^*\}$, which is a language over the ternary alphabet $\Sigma = \{0, 1, \#\}$. Similarly to the separation $Pal \notin REG/n$ [14], it is possible to prove that $Pal_{\#} \notin REG/n$, for instance, by employing a *swapping lemma* [14].

Since $Pal_{\#}$ is known to be in $DCFL$, the remaining task is to show that $Pal_{\#}$ belongs to $1RFA/Rn$. For simplicity, we assume that an input tape has no endmarkers. Our advice alphabet Γ is $\{0, 1, \#\}$ and our randomized advice D_n of size n is defined as follows. If $n = 2m$, then D_n generates a string $y\#y^R$ with probability 2^{-m} ; otherwise, D_n generates $\#^n$ with probability 1. Next, we define a *one-tape probabilistic finite automaton* (or a *1pfa*) $M = (Q, \Sigma, \delta, q_0, Q_{acc}, Q_{rej})$ with $Q_{acc} = \{q_0, q_2\}$, $Q_{rej} = \{q_1, q_3\}$, and $Q = Q_{acc} \cup Q_{rej}$. The transition function δ of M is defined as follows. For any bits $\sigma, \tau \in \{0, 1\}$ and any index $i \in \{0, 1\}$, we set $\delta(q_i, \begin{bmatrix} \sigma \\ \tau \end{bmatrix}) = q_{\sigma\tau+i \bmod 2}$ and $\delta(q_i, a) = q_{i+1 \bmod 2}$, where $a = \begin{bmatrix} \# \\ \# \end{bmatrix}$. For any other state/symbol pair (q, σ) , we make two new transitions from (q, σ) to both q_2 and q_3 with probability exactly $1/2$.

On any input of the form $x\#x'$, if $x' = x^R$, then M enters an accepting state using D_n with probability 1, where the probability is calculated according to transition probabilities of M as well as the probability distribution D_n . On the contrary, if $x' \neq x^R$, then M enters an accepting state with probability exactly

1/2, and thus an error probability is 1/2. To reduce this error probability to 1/4, we need to make two runs of the above procedure in parallel. It is not quite difficult to translate this 1pfa into an appropriate reversible automaton (by modifying randomized advice slightly), and we omit a detailed description of the desired 1rfa.

(2) In a way similar to (1), another language $Dup = \{ww \mid w \in \{0,1\}^*\}$ over the binary alphabet $\{0,1\}$ can be proven to fall into $1RFA/Rn$. Since Dup does not belong to CFL/n [14], the proposition instantly follows. \square

Proposition 4.3(2) strengthens the early result of $REG/Rn \not\subseteq CFL/n$ [15]. Here, we briefly discuss an immediate consequence of Proposition 4.3(2). If $1RFA/n = 1RFA/Rn$, then the obvious containment $1RFA/n \subseteq CFL/n$ leads to a conclusion $1RFA/Rn \subseteq CFL/n$; however, this contradicts Proposition 4.3(2). Therefore, we obtain a class separation between $1RFA/n$ and $1RFA/Rn$. This separation can be compared with $REG/n \neq REG/Rn$ [15].

Corollary 4.4 $1RFA/n \neq 1RFA/Rn$.

5 From Randomized Advice to Quantum Advice

In Section 3, we have studied the behaviors of 1rfa's that are augmented with randomized advice. In particular, we have shown in Corollary 4.4 that randomized advice is much more useful than deterministic advice for 1rfa's. In a similar fashion, we can supply randomized advice to assist 1qfa's and discuss how much randomized advice can enhance the recognition power of the 1qfa's. By extending randomized advice further to quantum advice, we will examine a situation surrounding 1qfa's in the presence of quantum advice and then consider how to make the most of the quantum advice to strengthen quantum computation.

5.1 Complexity of 1QFA/ Rn

Similar to $1RFA/Rn$, we will introduce an advised language family $1QFA/Rn$. A natural way is to define a language L to be in $1QFA/Rn$ if there exist a 1qfa M , a constant $\varepsilon \in [0, 1/2)$, an advice alphabet Γ , and an advice probability ensemble $\{D_n\}_{n \in \mathbb{N}}$ ($D_n : \Gamma^n \rightarrow [0, 1]$) such that (*) $\text{Prob}_{M, D_n}[M(\lfloor \frac{x}{D_n} \rfloor) = L(x)] \geq 1 - \varepsilon$ holds for every length $n \in \mathbb{N}$ and every string x of length n . Since M performs quantum operations, we need to state Condition (*) more precisely. Let $M = (Q, \Sigma_\Gamma, \{U_\sigma\}_{\sigma \in \Sigma_\Gamma}, q_0, Q_{acc}, Q_{rej})$ be any underlying 1qfa and let $\{D_n\}_{n \in \mathbb{N}}$ be an advice probability ensemble over Γ^* . Meanwhile, we assume that an input tape of M has no endmarkers. Let us define quantum states $|\phi_0^{(x,y)}\rangle = |q_0\rangle$ and $|\phi_i^{(x,y)}\rangle = T_{[\frac{\sigma_i}{\tau_i}]}|\phi_{i-1}^{(x,y)}\rangle$ in the space E_Q for any index $i \in [n]$, $x = \sigma_1\sigma_2 \cdots \sigma_n \in \Sigma^n$, and $y = \tau_1\tau_2 \cdots \tau_n \in \Gamma^n$. In the presence of randomized advice D_n , the acceptance probability $p_{acc}(x, D_n)$ of M on the input x is defined as $p_{acc}(x, D_n) = \sum_{y \in \Gamma^n} D_n(y) \sum_{i=1}^n \|P_{acc} U_{[\frac{\sigma_i}{\tau_i}]} |\phi_{i-1}^{(x,y)}\rangle\|^2$. In a similar way, the rejection probability $p_{rej}(x, D_n)$ is defined using P_{rej} in place of P_{acc} . With those notations, Condition (*) is now understood as stating that if $x \in L \cap \Sigma^n$ then $p_{acc}(x, D_n) \geq 1 - \varepsilon$ holds, and if $x \in \Sigma^n - L$ then $p_{rej}(x, D_n) \geq 1 - \varepsilon$ holds.

Let us start with a simple observation on a significance of the “bounded-error probability” requirement of 1qfa's. By augmenting $1QFA_{(a(n), b(n))}$ with randomized advice, we can define $1QFA_{(a(n), b(n))}/Rn$ as a generalization of $1QFA/Rn$. Recall from Section 1 that the notation “ALL” denotes the collection of all languages. When error bounds of 1qfa's become exactly 1/2, by an adequate choice of randomized advice, those 1qfa's can recognize all languages.

Lemma 5.1 $1QFA_{(1/2, 1/2)}/Rn = \text{ALL}$.

Proof. Let L be any language over alphabet Σ . We set our advice alphabet Γ to be $\Sigma \cup \{\#\}$, where $\#$ denotes a special symbol not in Σ . We intend to define a 1qfa $M = (Q, \Sigma_\Gamma, \{U_\sigma\}_{\sigma \in \Sigma_\Gamma}, q_0, Q_{acc}, Q_{rej})$ and randomized advice $\{D_n\}_{n \in \mathbb{N}}$.

Fix an arbitrary length $n \in \mathbb{N}$. For simplicity of the proof, assume that $n \geq 1$ and write L_n for the set $L \cap \Sigma^n$. In the case where $L_n = \emptyset$, D_n generates $\#^n$ with probability 1. By reading the first symbol in $\#^n$, M easily concludes that $L_n = \emptyset$, and thus it immediately rejects any input string. Next, assuming $L_n \neq \emptyset$, we set our randomized advice D_n as $D_n(y) = 1/|L_n|$ for any string $y \in L_n$ and $D_n(y) = 0$ for the other strings y . Our 1qfa M is designed to work as follows. Given each advice string s , (i) M checks whether its input $\lfloor \frac{x}{s} \rfloor$ satisfies $x = s$, (ii) if so, then M accepts the input with certainty, and (iii) otherwise, M accepts and rejects the input with equal probability.

To perform the above steps, we define $Q = \{q_0, q_1, q_3\}$, $Q_{acc} = \{q_1\}$, and $Q_{rej} = \{q_2\}$. The time-evolution operators $\{U_\sigma\}_{\sigma \in \Sigma_\Gamma}$ are defined as $U_\emptyset = U_{[\sigma]} = I$ (identity), and

$$U_{[\tau]} = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}, \quad U_{[\#]} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \text{and} \quad U_\$ = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $\sigma \neq \tau$. Note that an initial quantum state of M is $|q_0\rangle (= (1, 0, 0)^T)$. It is straightforward to verify that $x \in L_n$ iff $\text{Prob}_{M, D_n}[M(\lfloor \frac{x}{D_n} \rfloor) = 1] > 1/2$. Therefore, L belongs to $1\text{QFA}_{(1/2, 1/2)}/Rn$. \square

When deterministic advice is concerned, we have noted in Section 3, that $1\text{QFA}/n$ is contained in REG/n . As for randomized advice, a similar inclusion holds between $1\text{QFA}/Rn$ and REG/Rn although this fact is not obvious from their definitions.

Lemma 5.2 $1\text{QFA}/Rn \subseteq \text{REG}/Rn$.

Proof. Fix an input alphabet Σ and let L be any language in $1\text{QFA}/Rn$ over Σ . Let M be a 1qfa, Γ be an advice alphabet, and $\{D_n\}_{n \in \mathbb{N}}$ be an advice probability ensemble over Γ^* , and assume that, for every string $x \in \Sigma^n$, $\text{Prob}_{M, D_n}[M(\lfloor \frac{x}{D_n} \rfloor) = L(x)] \geq 1 - \varepsilon$ holds. In what follows, we fix $n \in \mathbb{N}$ and $x \in \Sigma^n$. Let us define $\Gamma^n = \{y_1, y_2, \dots, y_{c^n}\}$ with $c = |\Gamma|$. For each index $i \in [c^n]$, let $p_i = D_n(y_i)$ and $r_i = \text{Prob}_M[M(\lfloor \frac{x}{y_i} \rfloor) = L(x)]$ so that $\text{Prob}_{M, D_n}[M(\lfloor \frac{x}{D_n} \rfloor) = L(x)]$ is succinctly expressed as $\sum_{i=1}^{c^n} p_i r_i$.

Now, consider the set $A = \{i \in [c^n] \mid r_i \geq 1 - 3\varepsilon\}$. First, we want to show that $\sum_{i \in A} p_i \geq 2/3$. By the definitions of p_i 's and r_i 's, it follows that

$$\sum_{i=1}^{c^n} p_i r_i \leq \sum_{i \in A} p_i \cdot 1 + \sum_{i \notin A} p_i (1 - 3\varepsilon) \leq 1 - 3\varepsilon + 3\varepsilon \sum_{i \in A} p_i,$$

where the last inequality comes from $\sum_{i \notin A} p_i = 1 - \sum_{i \in A} p_i$. Since $\sum_i p_i r_i \geq 1 - \varepsilon$ by our assumption, we conclude that $\sum_{i \in A} p_i \geq 2/3$.

As shown in [7], we can translate the underlying 1qfa M into an appropriate “equivalent” 1dfa, say, N . This 1dfa N may not always produce the same output as the original 1qfa does with “high” probability; however, as far as we restrict our attention on the indices $i \in A$, N correctly outputs $L(x)$ using $\{D_n\}_{n \in \mathbb{N}}$ with probability at least $2/3$. Therefore, A belongs to REG/Rn . \square

As a direct consequence of Lemma 5.2 together with Proposition 4.3(1), the usefulness of randomized advice is shown below for 1qfa's.

Corollary 5.3 $1\text{QFA}/n \neq 1\text{QFA}/Rn$.

Proof. Assume that $1\text{QFA}/n = 1\text{QFA}/Rn$. In Proposition 4.3(1), we have shown that $1\text{RFA}/Rn \not\subseteq \text{REG}/n$. Since $1\text{RFA}/Rn \subseteq 1\text{QFA}/Rn$ by Lemma 5.2, it follows that $1\text{QFA}/Rn \not\subseteq \text{REG}/n$. Thus, our assumption leads to a conclusion that $1\text{QFA}/n \not\subseteq \text{REG}/n$. This contradicts the fact that $1\text{QFA}/n \subseteq \text{REG}/n$. Therefore, $1\text{QFA}/Rn$ is different from $1\text{QFA}/n$. \square

Since quantum computation handles quantum information, it is natural to consider a piece of advice, known as *quantum advice*, which is a series of (pure) quantum states. In the past literature, quantum advice has been discussed chiefly in the context of polynomial-time computations (see, e.g., [1, 10, 12]). Associated with an advice alphabet Γ , we denote by $|\phi_n\rangle$ a *normalized* quantum state in a Hilbert space of dimension $|\Gamma|^n$. Using a computational basis Γ^n , $|\phi_n\rangle$ can be expressed as a superposition of the form $\sum_{s \in \Gamma^n} \alpha_s |s\rangle$ with appropriate amplitudes $\alpha_s \in \mathbb{C}$ satisfying $\sum_{s \in \Gamma^n} |\alpha_s|^2 = 1$. For our later convenience, the succinct notation $|\lfloor \frac{x}{\phi_n} \rfloor\rangle$ indicates a particular quantum state $\sum_{s \in \Gamma^n} \alpha_s |\lfloor \frac{x}{s} \rfloor\rangle$ represented in computational basis $\Sigma_\Gamma^n = \{|\lfloor \frac{x}{s} \rfloor\rangle \mid x \in \Sigma^n, s \in \Gamma^n\}$.

To treat quantum advice formally, it is convenient to *rephrase* the earlier definition of advised 1qfa by expanding the original Hilbert space $E_Q = \text{span}\{|q\rangle \mid q \in Q\}$ used in Sections 3–5 to another Hilbert space $E_n = \text{span}\{|q\rangle|y\rangle \mid q \in Q, y \in \Gamma^n\}$, where n refers to “input size.” Three projection operators P_{acc} , P_{rej} , and P_{non} are appropriately modified to act on E_n . Notice that those operators are applied only to the first register containing inner states in Q . Given a specified index $i \in [n]$, a unitary operator $U_\sigma^{(i)}$ acting on the space E_n is applied to M 's inner state as well as the content of the i th tape cell (including both an input

symbol and an advice symbol). Since the input tape is *read-only*, although $U_\sigma^{(i)}$ accesses its second register containing advice strings in Γ^n , it cannot change the “content” of the second register. For such an operator $U_\sigma^{(i)}$, we set $T_\sigma^{(i)} = P_{\text{non}} U_\sigma^{(i)}$. Given a string $x = x_1 x_2 \cdots x_n$ of length n in Σ^* , an extended operator $T_x = T_{x_n}^{(n)} \cdots T_{x_2}^{(2)} T_{x_1}^{(1)}$ acts on E_n . On the input $x \in \Sigma^n$, an advised 1qfa M starts with an initial quantum state $|q_0\rangle|\phi_n\rangle = \sum_{y \in \Gamma^n} \alpha_y |q_0\rangle|y\rangle$. At time i , performing the measurement P_{acc} gives the acceptance probability $p_{\text{acc}}(x, \phi_n, i) = \left\| P_{\text{acc}} U_{x_i}^{(i)} T_{x_1 x_2 \cdots x_{i-1}} |q_0\rangle|\phi_n\rangle \right\|^2$, which equals $\left\| \sum_{y \in \Gamma^n} \alpha_y P_{\text{acc}} U_{x_i}^{(i)} T_{x_1 x_2 \cdots x_{i-1}} |q_0\rangle|y\rangle \right\|^2$. After the 1qfa halts, the (total) acceptance probability $p_{\text{acc}}(x, \phi_n)$ becomes $\sum_{i=1}^{n+2} p_{\text{acc}}(x, \phi_n, i)$. The rejection probabilities $p_{\text{rej}}(x, \phi_n, i)$ and $p_{\text{rej}}(x, \phi_n)$ are similarly calculated using P_{rej} in place of P_{acc} .

Unlike a model of quantum Turing machine, our current model of 1qfa is equipped with two *read-only* tape tracks and this “read-only” restriction severely limits the potential power of quantum advice. To understand this situation, let us observe that advice strings in a given quantum advice state are unaltered and that quantum computations associated with different advice strings never interfere with one another. This observation leads to the following claim. For succinctness, we use the notation $\text{Prob}_M[M(\lfloor \phi_{|x|}^x \rfloor) = L(x)]$ to denote the total probability of M on input $\lfloor \phi_{|x|}^x \rfloor$ producing output value $L(x)$.

Proposition 5.4 *Let L be any language over alphabet Σ . The following two statements are logically equivalent.*

1. $L \in \text{1QFA}/Rn$.
2. *There exist a 1qfa M with read-only tape tracks, an advice alphabet Γ , a series $\Phi = \{|\phi_n\rangle\}_{n \in \mathbb{N}}$ of quantum advice states over Γ^* , and an error bound $\varepsilon \in [0, 1/2)$ satisfying $\text{Prob}_M[M(\lfloor \phi_{|x|}^x \rfloor) = L(x)] \geq 1 - \varepsilon$ for any input $x \in \Sigma^*$.*

Proof. (1 \Rightarrow 2) Note that a piece of randomized advice, say, D_n over Γ^n can be embedded into the aforementioned Hilbert space E_n as a quantum state of the form $|\phi_n\rangle = \sum_{y \in \Gamma^n} \sqrt{D_n(y)} |y\rangle$. Statement (2) thus follows immediately by replacing D_n with $|\phi_n\rangle$.

(2 \Rightarrow 1) Take M , Γ , Φ , and ε described in the lemma. Let $n \in \mathbb{N}$. For each advice quantum state $|\phi_n\rangle \in \Phi$, assume that $|\phi_n\rangle = \sum_{y \in \Gamma^n} \alpha_y |y\rangle$ for appropriate amplitudes $\alpha_i \in \mathbb{C}$. To make our argument simple, we assume that our input tape has no endmarkers. Let $x = \sigma_1 \sigma_2 \cdots \sigma_n$ be any string in Σ^n . Choose an appropriate string $y = \tau_1 \tau_2 \cdots \tau_n$ of length n . For the pair (x, y) , we define $|\phi_0^{(x, y)}\rangle = |q_0\rangle|y\rangle$ and $|\phi_i^{(x, y)}\rangle = T_{\sigma_i}^{(i)} |\phi_{i-1}^{(x, y)}\rangle$ for each index $i \in [n]$. As remarked earlier, $T_{\sigma_i}^{(i)}$ modifies only M ’s inner state; thus, $|\phi_i^{(x, y)}\rangle$ can be expressed as $|\psi_i^{(x, y)}\rangle|y\rangle$. For convenience, let $|\tilde{\phi}_i^{(x, y)}\rangle = U_{\sigma_i}^{(i)} |\phi_{i-1}^{(x, y)}\rangle$, which is also written as $|\tilde{\psi}_i^{(x, y)}\rangle|y\rangle$. The total acceptance probability $p_{\text{acc}}(x, \phi_n)$ is calculated as

$$p_{\text{acc}}(x, \phi_n) = \left\| \sum_{y \in \Gamma^n} |\alpha_y|^2 \sum_{i=1}^n P_{\text{acc}} U_{\sigma_i}^{(i)} |\phi_{i-1}^{(x, y)}\rangle \right\|^2 = \sum_{y \in \Gamma^n} |\alpha_y|^2 \left\| \sum_{i=1}^n P_{\text{acc}} |\tilde{\psi}_i^{(x, y)}\rangle|y\rangle \right\|^2.$$

The rejection probability $p_{\text{rej}}(x, \phi_n)$ is also calculated similarly by replacing P_{acc} with P_{rej} . To obtain the desired consequence, it suffices to take an advice probability ensemble $\{D_n\}_{n \in \mathbb{N}}$ defined as $D_n(y) = |\alpha_y|^2$ for each string $y \in \Gamma^n$. \square

Proposition 5.4 indicates that, if a 1qfa has only read-only tape tracks, then the power of quantum advice is reduced to that of randomized advice. The proposition therefore leads us to an introduction of a notion of “rewritable” advice tracks in the next subsection.

5.2 Making the Most of Quantum Advice

We begin with a brief discussion on a simple and natural extension of the original 1qfa model. First of all, we remind that, for most types of classical one-way finite automata, it is of no importance whether a tape head erases or modifies the content of any tape cell before leaving off that tape cell, because the tape head never returns to this tape cell to retrieve any modified information. In those cases, although the tape head is allowed to return to the modified tape cells, the computational power of automata do not change. For instance, as noted earlier, advised 1dfa’s are computationally equivalent to one-tape linear-time deterministic Turing machines with linear-size advice; namely, $1\text{-DLIN}/lin = \text{REG}/n$ and $1\text{-BPLIN}/Rlin = \text{REG}/Rn$ hold [13, 15]. These equalities suggest that the “read-only” requirement of an input tape is irrelevant to the

computational power of 1dfa's. Now, suppose that we re-define two automata models—1dfa's and 1rfa's—used in the previous sections for deterministic and randomized advice so that they are allowed to modify any *advice symbol* written in any tape cell of the lower tape track before their tape heads leave the scanned tape cell (but the tape heads never visit the same tape cell again). For our reference, such a tape track is referred to as a *rewritable advice tape track*. It is not difficult to see that such a re-definition does not alter the advised language families, such as REG/n , $\text{1RFA}/n$, REG/Rn , and $\text{1RFA}/Rn$.

When quantum advice is concerned, what would happen if we use 1qfa's with rewritable advice tape tracks? For our convenience, we call by a *rewritable 1qfa* such a 1qfa that can access a rewritable advice tape track. For simplicity, we assume that an upper track that holds a standard input string is still read-only as in the original model of 1qfa's. Notice that what actually limits the power of 1qfa's is a prohibition of disposing of (or dumping) quantum information after it is read and its information is processed. Therefore, quantum computation may draw a considerable benefit from a modification of advice strings, despite the fact that a one-way head move still hampers the machine's ability.

Let us recall the rephrased description of advised 1qfa's presented in Section 5.1. Using the same notations, a rewritable 1qfa $M = (Q, \Sigma_\Gamma, \{U_\sigma^{(i)}\}_{\sigma \in \Sigma_\Gamma, i \in \mathbb{N}}, q_0, Q_{acc}, Q_{rej})$ starts with an initial quantum state $|q_0\rangle|\phi_n\rangle$, where $|\phi_n\rangle$ is an advice quantum state in $\text{span}\{|z\rangle \mid z \in \Gamma^n\}$ when a string x of length n is given as a standard input. A unary operator $U_{x_i}^{(i)}$ is still applied to only M 's inner states and the content of the i th tape cell; however, it now freely modifies the content of the tape cell. The acceptance probability $p_{acc}(x, \phi_n)$ of M on x with the quantum advice $|\phi_n\rangle$ is the sum, over all $i \in [n]$, of $\|P_{acc}U_{x_i}^{(i)}T_{x_1x_2\cdots x_{i-1}}|q_0\rangle|\phi_n\rangle\|^2$. The rejection probability $p_{rej}(x, \phi_n)$ is similarly defined. To emphasize a use of quantum advice, a special notation $\text{1QFA}^*/Qn$ will be used to denote the family of all languages recognized with bounded-error probability by rewritable 1qfa's using quantum advice.

The actual power of rewritable 1qfa's equipped with quantum advice is exemplified in Lemma 5.5. For the proposition, let us review the language family 1-BQLIN , which was introduced in [13] as the family of all languages recognized by one-tape two-way one-head off-line quantum Turing machines whose error probabilities are upper-bounded by $1/4$, where all the (classically-viewed) computation paths generated by the machines must terminate simultaneously within a *linear* number of steps. Appending linear-size quantum advice to those machines, we naturally expand 1-BQLIN to its advised version $\text{1-BQLIN}/Qlin$, which is also seen as a quantum analogue of $\text{1-BPLIN}/Rlin$. Due to a nature of Turing machine, during its computation, the machine can freely alter not only a given advice string but also a given input string.

We will show a location of $\text{1QFA}^*/Qn$ in a landscape of low-complexity classes.

Lemma 5.5 $\text{REG}/Rn \subseteq \text{1QFA}^*/Qn \subseteq \text{1-BQLIN}/Qlin$.

Proof. The second containment $\text{1QFA}^*/Qn \subseteq \text{1-BQLIN}/Qlin$ is obvious, since a 1qfa can be viewed as a special case of one-tape quantum Turing machine that satisfies the requirements described above.

The first containment $\text{REG}/Rn \subseteq \text{1QFA}^*/Qn$ is shown, roughly with a similar idea used in, e.g., [11, Proposition 4.2], by dumping the information on a current inner state of an underlying 1dfa onto a rewritable advice track in order to turn a deterministic move into a quantum move.

More precisely, take any language S in REG/Rn . There are a 1dfa M , an advice alphabet Γ , an advice probability ensemble $\{D_n\}_{n \in \mathbb{N}}$, an error bound $\varepsilon \in [0, 1/2)$ such that $\text{Prob}_{M, D_n}[M(\lfloor \frac{x}{D_n} \rfloor) = S(x)] \geq 1 - \varepsilon$ holds for every length $n \in \mathbb{N}$ and every string $x \in \Sigma^n$. We will construct a rewritable 1qfa N as follows. In an arbitrary configuration, assume that M is in inner state q , scanning $\lfloor \frac{\sigma}{\tau} \rfloor$, and applies a transition $\delta(q, \lfloor \frac{\sigma}{\tau} \rfloor) = q'$. Corresponding to this configuration, N scans $\lfloor \frac{\sigma}{\tau} \rfloor$ in inner state q , modifies $\lfloor \frac{\sigma}{\tau} \rfloor$ to $\lfloor \frac{\sigma}{\tau_q} \rfloor$, where $\tau_q = \lfloor \frac{\sigma}{\tau} \rfloor$ is a new advice symbol. Note that, for each fixed advice string $y \in \Gamma^n$, M accepts $\lfloor \frac{x}{y} \rfloor$ iff N on input $\lfloor \frac{x}{y} \rfloor$ enters an accepting state with probability 1. As our quantum advice, we use the quantum state $|\phi_n\rangle = \sum_{y \in \Gamma^n} \sqrt{D_n(y)}|y\rangle$. This implies that $\text{Prob}_N[N(\lfloor \frac{x}{\phi_n} \rfloor) = S(x)] = \text{Prob}_{M, D_n}[M(\lfloor \frac{x}{D_n} \rfloor) = S(x)]$. Therefore, S is in $\text{1QFA}^*/Qn$. \square

An introduction of rewritable advice track also makes it possible to prove a *closure property* of $\text{1QFA}^*/Qn$ under Boolean operations. In contrast, some of those properties are not known to hold for 1QFA , chiefly because a 1qfa cannot, in general, amplify its success probability.

Proposition 5.6 *The advised language family $\text{1QFA}^*/Qn$ is closed under union, intersection, and complementation.*

The closure properties of $\text{1QFA}^*/Qn$ given in Proposition 5.6 are a direct consequence of the facts shown in Lemmas 5.7 and 5.8 that, by an appropriate use of quantum advice, (i) a rewritable 1qfa can reduce

the number of applications of measurement operations down to one and (ii) the 1qfa can reduce its error probability as well.

As shown in the next lemma, a use of rewritable tape tracks makes it possible to postpone all (projection) measurement operations to the end of their computation, and thus it simplifies the behaviors of 1qfa's significantly.

Lemma 5.7 *For any rewritable 1qfa M with quantum advice $\Psi = \{|\phi_n\rangle\}_{n \in \mathbb{N}}$, there exist another rewritable 1qfa N and another quantum advice $\Psi' = \{|\phi'_n\rangle\}_{n \in \mathbb{N}}$ such that (i) N conducts a measurement only once just after scanning an entire input and (ii) after the measurement, the acceptance probability of N on each input with Ψ' equals the acceptance probability of M on the same input with Ψ .*

An error bound of each 1qfa can be significantly reduced with a help of quantum advice. This is quite useful in constructing desired 1qfa's that recognize given target languages.

Lemma 5.8 *Let L be any language over alphabet Σ in $1QFA^*/Qn$. For any constant $\varepsilon \in (0, 1/2)$, there exist a rewritable 1qfa M and a series $\{|\phi_n\rangle\}_{n \in \mathbb{N}}$ of quantum advice states such that, for every length $n \in \mathbb{N}$, (i) for any string $x \in L \cap \Sigma^n$, M accepts $[[\frac{x}{\phi_n}]]$ with probability at least $1 - \varepsilon$, and (iii) for any string $x \in \Sigma^n - L$, M rejects $[[\frac{x}{\phi_n}]]$ with probability at least $1 - \varepsilon$.*

Before proving Lemmas 5.7 and 5.8, we will present the proof of Proposition 5.6.

Proof of Proposition 5.6. We will show three closure properties of $1QFA^*/Qn$. Let L_1 and L_2 be two arbitrary languages in $1QFA^*/Qn$. For each index $i \in \{1, 2\}$, let $M_i = (Q_i, \Sigma_{\Gamma_i}, \{U_{i,\sigma}\}_{\sigma \in \Sigma_{\Gamma_i}}, q_{i,0}, Q_{i,acc}, Q_{i,rej})$ be a rewritable 1qfa that recognizes L_i with quantum advice $\Phi_i = \{|\phi_{i,n}\rangle\}_n$ over advice alphabet Γ_i with error bound ε_i . For simplicity, we assume that each M_i has no left endmarker \dagger and that M_i performs no measurement until reading the right endmarker $\$$. Without loss of generality, we assume that $\Gamma_1 = \Gamma_2$ and simply write Γ for Γ_1 . We also assume that $|\phi_{i,n}\rangle = \sum_{y \in \Gamma} \alpha_y^{(i)} |y\rangle$ for each index $i \in \{1, 2\}$.

[Complementation] Consider the complement of L_1 . Since M_1 recognizes L_1 using Φ_1 with bounded-error probability, we modify M_1 by exchanging the roles of “accepting states” and “rejecting states” in Q . This is possible because M_1 conducts a measurement only once at the end of its computation. It is therefore obvious that this new machine recognizes L_1 using Φ_1 with the same success probability.

[Intersection] By Lemma 5.8, it is possible to assume that $0 \leq \varepsilon_i < 1 - \frac{\sqrt{2}}{2}$. For convenience, we set $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_1 \varepsilon_2$. By the choice of ε_i 's, it follows that $0 \leq \varepsilon < 1/2$.

Let us define a new rewritable 1qfa M as follows. Let $q_0 = (q_{1,0}, q_{2,0})$, $Q = Q_1 \times Q_2$, $Q_{acc} = Q_{1,acc} \times Q_{2,acc}$, and $Q_{rej} = (Q_{1,rej} \times Q) \cup (Q \times Q_{2,rej})$. Each operator U_σ is defined as $U_\sigma |q_1, q_2\rangle |y_1, y_2\rangle = U_{1,\sigma} |q_1\rangle |y_1\rangle \otimes U_{2,\sigma} |q_2\rangle |y_2\rangle$. We set $T_x^{(n)} = U_{x_n} U_{x_{n-1}} \cdots U_{x_1}$. Now, we prepare new quantum advice $|\psi_n\rangle$ of the form $|\phi_{1,n}\rangle \otimes |\phi_{2,n}\rangle$. When M reads the input string, M generates a quantum state $T_x^{(n)} |q_0\rangle |\psi_n\rangle = T_{1,x}^{(n)} |q_{1,0}\rangle |\phi_{1,n}\rangle \otimes T_{2,x}^{(n)} |q_{2,0}\rangle |\phi_{2,n}\rangle$, where $T_{i,x}^{(n)} = U_{i,x_n} U_{i,x_{n-1}} \cdots U_{i,x_1}$ for each index $i \in \{1, 2\}$. Because M 's computation is essentially decomposed into two independent computations of M_1 and M_2 , it is easy to show that

$$\text{Prob}_M[M([\frac{x}{\psi_n}]) = 1] = \text{Prob}_{M_1}[M_1([\frac{x}{\phi_{1,n}}]) = 1] \cdot \text{Prob}_{M_2}[M_2([\frac{x}{\phi_{2,n}}]) = 1]. \quad (1)$$

From this equality, we obtain the following.

- (1) If $x \in L$, then it holds by Eq.(1) that $\text{Prob}_M[M([\frac{x}{\psi_n}]) = 1] \geq (1 - \varepsilon_1)(1 - \varepsilon_2) = 1 - \varepsilon$.
- (2) If $x \notin L$, then it holds that $\text{Prob}_M[M([\frac{x}{\psi_n}]) = 0] \geq \max\{1 - \varepsilon_1, 1 - \varepsilon_2\} \geq 1 - \varepsilon$, because $\varepsilon \geq \max\{\varepsilon_1, \varepsilon_2\}$ holds.

Therefore, M recognizes L using the advice $|\psi_n\rangle$ with bounded-error probability.

[Union] Since $L_1 \cup L_2 = \overline{\overline{L_1} \cap \overline{L_2}}$, this “union” case follows from the previous cases of “complementation” and “intersection.” \square

To finish the proof of Proposition 5.6, we will prove Lemmas 5.7 and 5.8. Lemma 5.7 is shown intuitively as follows. Instead of measuring 1qfa's inner states at every step, we write them down on an advice track and enter new (but corresponding) non-halting states so that we can wait without performing any measurement until the last-minute measurement at the end of a computation of the 1qfa.

Proof of Lemma 5.7. Let Σ and Γ denote respectively an input alphabet and an advice alphabet. Let $M = (Q, \Sigma_\Gamma, \{U_\sigma^{(i)}\}_{\sigma \in \Sigma_\Gamma, i \in \mathbb{N}^+}, q_0, Q_{acc}, Q_{rej})$ be any rewritable 1qfa and let $\Phi = \{|\phi_n\rangle\}_{n \in \mathbb{N}}$ be a series

of advice quantum states whose advice alphabet is Γ . For simplicity, we assume that an input tape has no endmarkers. Let $p_{acc}(x, \phi_n, i)$ denote the acceptance probability of M on input x at time i ; that is, $p_{acc}(x, \phi_n, i) = \|P_{acc}U_{x_i}T_{x_1x_2\cdots x_{i-1}}|q_0\rangle|\phi_n\rangle\|^2$.

First, by modifying M , we define a new rewritable 1qfa $N = (\tilde{Q}, \Sigma_{\tilde{\Gamma}}, \{\hat{U}_{\sigma}^{(i)}\}_{\sigma \in \Sigma_{\tilde{\Gamma}}, i \in \mathbb{N}^+}, q_0, Q_{acc}, Q_{rej})$ that conducts a measurement only once just after reading the entire input. To each halting state $q \in Q_{halt}$, we assign a new *non-halting* state \hat{q} , and we then define $\hat{Q}_{halt} = \{\hat{q} \mid q \in Q_{halt}\}$. A new set of inner states is $\tilde{Q} = Q \cup \hat{Q}_{halt}$. Our new advice alphabet is $\tilde{\Gamma} = \Gamma \cup \Gamma' \cup \{[\frac{s}{\tau}] \mid \tau \in \Gamma\}$, where $\Gamma' = \{[\frac{\hat{q}}{\tau}] \mid \hat{q} \in \hat{Q}_{halt}, \tau \in \Gamma\}$, and new quantum advice Ψ' consists of quantum states $|\phi_n^s\rangle = \sum_{y \in \Gamma^n} \gamma_y |y_1 y_2 \cdots y_{n-1} [\frac{s}{y_n}]\rangle$ for each $|\phi_n\rangle = \sum_{y \in \Gamma^n} \gamma_y |y\rangle$, provided that each y has the form $y = y_1 y_2 \cdots y_n$. The operators $\hat{U}_{\sigma}^{(i)}$ of N will be defined later.

Similar to $|\phi_n^s\rangle$, if $|\psi\rangle$ is expressed in the form $\sum_{q \in Q} \sum_{y \in \Gamma^n} \alpha_{q,y} |q\rangle |y_1 y_2 \cdots y_{n-1} y_n\rangle$ with $y = y_1 y_2 \cdots y_{n-1} y_n$, then $|\psi^s\rangle$ denotes the quantum state $\sum_{q \in Q} \sum_{y \in \Gamma^n} \alpha_{q,y} |q\rangle |y_1 y_2 \cdots y_{n-1} [\frac{s}{y_n}]\rangle$. Initially, M is in quantum state $|\psi_0\rangle = |q_0\rangle|\phi_n\rangle$ with Φ , and N with Φ' is in $|\psi'_0\rangle = |q_0\rangle|\phi_n^s\rangle$, which equals $|\psi_0^s\rangle + |\xi_0\rangle$, where $|\xi_0\rangle = 0$. Now, assume that, at time $i - 1 \geq 0$ ($i \leq n$), M is in quantum state $|\psi_{i-1}\rangle \in E_{non}$ and N is in $|\psi'_{i-1}\rangle = |\psi_{i-1}^s\rangle + |\xi_{i-1}\rangle$, where $|\xi_{i-1}\rangle \in E'_n$, where $E'_n = span\{|q\rangle|y\rangle \mid q \in \hat{Q}_{halt}, y \in \Gamma^n\}$. Let us consider the i -th step. Assume that, before performing a measurement, M generates a quantum state $U_{x_i}^{(i)}|\psi_{i-1}\rangle = |\psi_i\rangle + |\psi_{i,acc}\rangle + |\psi_{i,rej}\rangle \in E_{non} \oplus E_{acc} \oplus E_{rej}$. After the measurement, the acceptance probability $p_{acc}(x, \phi_n, i)$ becomes $\| |\psi_{i,acc}\rangle \|^2$.

Next, we will define a unitary operator $\hat{U}_{x_i}^{(i)}$. Corresponding to $|\psi_{i,acc}\rangle$, set $|\psi'_{i,acc}\rangle = \sum_{q \in Q_{acc}} \sum_{y \in \Gamma^n} \alpha_{q,y} |q\rangle |y_1 \cdots y_{i-1} [\frac{q}{y_i}] y_{i+1} \cdots y_{n-1} [\frac{s}{y_n}]\rangle$ if $|\psi_{i,acc}\rangle = \sum_{q \in Q_{acc}} \sum_{y \in \Gamma^n} \alpha_{q,y} |q\rangle |y_1 \cdots y_n\rangle$. Similarly, $|\psi'_{i,rej}\rangle$ is defined. The $\hat{U}_{x_i}^{(i)}$ is defined to satisfy $\hat{U}_{x_i}^{(i)}|\psi_{i-1}^s\rangle = |\psi_i^s\rangle + |\psi'_{i,acc}\rangle + |\psi'_{i,rej}\rangle$. Moreover, when $\hat{q} \in \hat{Q}_{halt}$, we define $\hat{U}_{x_i}^{(i)}|\hat{q}\rangle |y'_1 \cdots y'_{i-1} y_i y_{i+1} \cdots y_n\rangle = |\hat{q}\rangle |y'_1 \cdots y'_{i-1} [\frac{\hat{q}}{y_i}] y_{i+1} \cdots y_n\rangle$, where $y'_1, \dots, y'_{i-1} \in \Gamma'$ and $y_i, \dots, y_n \in \Gamma$. The machine N therefore generates

$$|\psi'_i\rangle = \hat{U}_{x_i}^{(i)}|\psi'_{i-1}\rangle = \hat{U}_{x_i}^{(i)}|\psi_{i-1}^s\rangle + \hat{U}_{x_i}^{(i)}|\xi_{i-1}\rangle = |\psi_i^s\rangle + |\psi'_{i,acc}\rangle + |\psi'_{i,rej}\rangle + \hat{U}_{x_i}^{(i)}|\xi_{i-1}\rangle.$$

Finally, we set $|\xi_i\rangle$ to be $|\psi'_{i,acc}\rangle + |\psi'_{i,rej}\rangle + \hat{U}_{x_i}^{(i)}|\xi_{i-1}\rangle$, which belongs to E'_n . Since $\| |\psi_{i,acc}\rangle \| = \| |\psi'_{i,acc}\rangle \|$, we obtain $p_{acc}(x, \phi_n, i) = \| |\psi'_{i,acc}\rangle \|^2$. It is important to note that every vector $|\xi_i\rangle$ is orthogonal to $|\xi_{i-1}\rangle$ because N generates different strings on its rewritable advice tape track at time i .

At the final step, since we need to prepare for a measurement, we define $\hat{U}_{x_n}^{(n)}$ to satisfy $\hat{U}_{x_n}^{(n)}|\psi_{n-1}^s\rangle = \sum_{q \in Q} \sum_{y \in \Gamma^n} |q\rangle |y_1 \cdots y_{n-1} [\frac{q}{y_n}]\rangle$ if $U_{x_n}^{(n)}|\psi_{n-1}\rangle = \sum_{q \in Q} \sum_{y \in \Gamma^n} |q\rangle |y_1 \cdots y_{n-1} y_n\rangle$. For every $\hat{q} \in \hat{Q}_{halt}$, we define $\hat{U}_{x_n}^{(n)}|\hat{q}\rangle |y'_1 \cdots y'_{n-1} [\frac{s}{y_n}]\rangle = |q\rangle |y'_1 \cdots y'_{n-1} [\frac{\hat{q}}{y_n}]\rangle$, where $y'_1, \dots, y'_{n-1} \in \Gamma'$ and $y_n \in \Gamma$. The acceptance probability $p_{acc}(x, \phi_n, n)$ of M at time n , which is $\|P_{acc}U_{x_n}^{(n)}|\psi_{n-1}\rangle\|^2$, equals $\|P_{acc}\hat{U}_{x_n}^{(n)}|\psi_{n-1}^s\rangle\|^2$. Note that $P_{acc}\hat{U}_{x_n}^{(n)}|\psi'_{n-1}\rangle = P_{acc}\hat{U}_{x_n}^{(n)}|\psi_{n-1}^s\rangle + \sum_{i=1}^{n-1} P_{acc}\hat{U}_{x_n}^{(n)} \cdots \hat{U}_{x_{i+1}}^{(i+1)}|\psi'_{i,acc}\rangle$. After the measurement, since $\|P_{acc}\hat{U}_{x_n}^{(n)} \cdots \hat{U}_{x_{i+1}}^{(i+1)}|\psi'_{i,acc}\rangle\| = \| |\psi'_{i,acc}\rangle \|$, N produces the total acceptance probability $p = \sum_{i=1}^{n-1} \| |\psi'_{i,acc}\rangle \|^2 + \|P_{acc}\hat{U}_{x_n}^{(n)}|\psi_{n-1}^s\rangle\|^2$. Since $\|P_{acc}\hat{U}_{x_n}^{(n)}|\psi_{n-1}^s\rangle\|^2 = \|P_{acc}U_{x_n}^{(n)}|\psi_{n-1}\rangle\|^2 = p_{acc}(x, \phi_n, n)$ and $\| |\psi'_{i,acc}\rangle \|^2 = p_{acc}(x, \phi_n, i)$ for all $i \in [n-1]$, we conclude that p equals $p_{acc}(x, \phi_n)$ of M . \square

To complete the proof of Proposition 5.6, we still need to prove Lemma 5.8. The proof of the lemma is based on a technique of *parallel repetition* of the same quantum computation, and Lemma 5.7 actually helps make the parallel repetition technique applicable. For completeness, we include the proof of the lemma although it involves a standard “majority vote” argument.

Proof of Lemma 5.8. Since $L \in 1QFA^*/Qn$, we take a rewritable 1qfa M , an error bound ε_0 , and a series $\Psi = \{|\phi_n\rangle\}_{n \in \mathbb{N}}$ of quantum advice states such that $\text{Prob}_M[M([\frac{x}{\phi_n}]) = L(x)] \geq 1 - \varepsilon_0$ for every length $n \in \mathbb{N}$ and every string $x \in \Sigma^n$. For a later reference, we write ε_x for the value $1 - \text{Prob}_M[M([\frac{x}{\phi_n}]) = L(x)]$. Choose an arbitrary error bound $\varepsilon \in (0, 1/2)$. Lemma 5.7 lets M conduct a measurement only once at the end of its computation.

If $\varepsilon_0 \leq \varepsilon$, then M obviously outputs $L(x)$ with probability at least $1 - \varepsilon_0 \geq 1 - \varepsilon$, and thus the lemma is true. Therefore, in what follows, we consider the case where $0 < \varepsilon < \varepsilon_0$. Depending on the value ε , we will select an odd number k , which indicates the number of times we do in parallel the execution of M on each input x . As for the number k , we choose the minimal odd number satisfying that $1 -$

$$\sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{\lfloor k/2 \rfloor + i} \varepsilon_0^{\lfloor k/2 \rfloor - i} (1 - \varepsilon_0)^{\lfloor k/2 \rfloor + i} \leq \varepsilon.$$

We prepare a new set Q' of inner states as the collection of all k -tuples $(q_{i_1}, q_{i_2}, \dots, q_{i_k}) \in Q^k$. We wish to express those k -tuples using k different registers $|q_{i_1}\rangle|q_{i_2}\rangle \cdots |q_{i_k}\rangle$. Now, we simulate M by a new rewritable 1qfa M' in the following manner. On input x , M' runs M on each of the k registers simultaneously in parallel. In the end of computation, if the k registers contain a basis vector $|q_{i_1}\rangle|q_{i_2}\rangle \cdots |q_{i_k}\rangle$ for certain indices i_1, i_2, \dots, i_k , then M' enters a new inner state $q^{(i_1, i_2, \dots, i_k)}$. Let Q'_{fin} denote the set of all such new inner states. Next, we will partition Q'_{fin} into three subsets, Q'_{acc} , Q'_{rej} , and Q'_{other} . Let Q'_{acc} (resp., Q'_{rej}) be composed of all inner states $q^{(i_1, i_2, \dots, i_k)}$ for which $|\{i \in [k] \mid q_i \in Q_{acc}\}| \geq \lceil k/2 \rceil$ (resp., $|\{i \in [k] \mid q_i \in Q_{rej}\}| \geq \lceil k/2 \rceil$) and let $Q'_{other} = Q'_{fin} - Q'_{acc} \cup Q'_{rej}$. For each string x , the probability that M' successfully produces $L(x)$ equals $\sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{\lfloor k/2 \rfloor + i} \varepsilon_x^{\lfloor k/2 \rfloor - i} (1 - \varepsilon_x)^{\lfloor k/2 \rfloor + i}$, which exceeds $\sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{\lfloor k/2 \rfloor + i} \varepsilon_0^{\lfloor k/2 \rfloor - i} (1 - \varepsilon_0)^{\lfloor k/2 \rfloor + i}$ since $\varepsilon_x \leq \varepsilon_0$. By the choice of k , M' recognizes L with success probability at least $1 - \varepsilon$. \square

Appendix: Proof of Lemma 3.1

This appendix gives the proof of Lemma 3.1 that has been omitted in Section 3 for readability.

Let Σ be any alphabet. Let $M = (Q, \Sigma, \{U_\sigma\}_{\sigma \in \tilde{\Sigma}}, q_0, Q_{acc}, Q_{rej})$ be any 1qfa, where $\tilde{\Sigma} = \Sigma \cup \{\$, \#\}$. In what follows, let $x = x_1 x_2 \cdots x_n$ be any string of length n in $\tilde{\Sigma}^*$, let $|\phi\rangle$ and $|\phi'\rangle$ be any two quantum states in E_{non} and let $\psi = (|\phi\rangle, \gamma_1, \gamma_2)$ and $\psi' = (|\phi'\rangle, \gamma'_1, \gamma'_2)$ be any two elements in \mathcal{S} . Let $T_\sigma = P_{non} U_\sigma$ for each symbol $\sigma \in \tilde{\Sigma}$ and set $T_x = T_{x_n} T_{x_{n-1}} \cdots T_{x_2} T_{x_1}$. In addition, for each index $i \in [n]$, we define $|\phi_i\rangle = T_{x_1 x_2 \cdots x_{i-1}} |\phi\rangle$ and $|\phi'_i\rangle = T_{x_1 x_2 \cdots x_{i-1}} |\phi'\rangle$. Note that $|\phi_1\rangle = |\phi\rangle$ and $|\phi'_1\rangle = |\phi'\rangle$ hold. Finally, we set $\alpha_i = \|P_{acc} U_{x_i} |\phi_i\rangle\|^2$ and $\beta_i = \|P_{rej} U_{x_i} |\phi_i\rangle\|^2$; similarly, we define α'_i and β'_i using $|\phi'_i\rangle$ in place of $|\phi_i\rangle$.

Before presenting the proof of Lemma 3.1, we will list four useful properties.

- Claim 11**
1. $\| |\phi\rangle \|^2 = \|T_x |\phi\rangle\|^2 + \sum_{i=1}^n \alpha_i + \sum_{i=1}^n \beta_i$.
 2. $\| |\phi\rangle - |\phi'\rangle \|^2 = \|T_x (|\phi\rangle - |\phi'\rangle)\|^2 + \sum_{i=1}^n \|P_{acc} U_{x_i} (|\phi_i\rangle - |\phi'_i\rangle)\|^2 + \sum_{i=1}^n \|P_{rej} U_{x_i} (|\phi_i\rangle - |\phi'_i\rangle)\|^2$.
 3. $2\| |\phi\rangle - |\phi'\rangle \|^2 - 2\|T_x (|\phi\rangle - |\phi'\rangle)\|^2 \geq |\sum_{i=1}^n (\alpha_i - \alpha'_i)| + |\sum_{i=1}^n (\beta_i - \beta'_i)|$.
 4. $2\langle |\phi\rangle | \phi'\rangle - \langle T_x |\phi\rangle | T_x |\phi'\rangle \rangle \leq (\| |\phi\rangle \|^2 - \|T_x |\phi\rangle\|^2) + (\| |\phi'\rangle \|^2 - \|T_x |\phi'\rangle\|^2)$.

Proof. (1) It holds that $U_{x_i} = T_{x_i} + P_{acc} U_{x_i} + P_{rej} U_{x_i}$ for each index $i \in [n]$. Since $U_{x_i}^\dagger U_{x_i} = I$, it thus follows that

$$\| |\phi_i\rangle \|^2 = \|U_{x_i} |\phi_i\rangle\|^2 = \|P_{acc} U_{x_i} |\phi_i\rangle\|^2 + \|P_{rej} U_{x_i} |\phi_i\rangle\|^2 + \|T_{x_i} |\phi_i\rangle\|^2. \quad (2)$$

Applying this equality repeatedly, we obtain

$$\begin{aligned} \| |\phi\rangle \|^2 &= \| |\phi_2\rangle \|^2 + \|P_{acc} U_{x_1} |\phi_1\rangle\|^2 + \|P_{rej} U_{x_1} |\phi_1\rangle\|^2 \\ &= \| |\phi_3\rangle \|^2 + \sum_{i=1}^2 \|P_{acc} U_{x_i} |\phi_i\rangle\|^2 + \sum_{i=1}^2 \|P_{rej} U_{x_i} |\phi_i\rangle\|^2 \\ &= \dots\dots\dots \\ &= \| |\phi_{n+1}\rangle \|^2 + \sum_{i=1}^n \|P_{acc} U_{x_i} |\phi_i\rangle\|^2 + \sum_{i=1}^n \|P_{rej} U_{x_i} |\phi_i\rangle\|^2. \end{aligned}$$

The desired formula immediately follows since $T_x |\phi\rangle = |\phi_{n+1}\rangle$, $\alpha_i = \|P_{acc} U_{x_i} |\phi_i\rangle\|^2$, and $\beta_i = \|P_{rej} U_{x_i} |\phi_i\rangle\|^2$.

(2) This is obtained by an argument similar to (1) using the equality

$$\| |\phi_i\rangle - |\phi'_i\rangle \|^2 = \|T_{x_i} (|\phi_i\rangle - |\phi'_i\rangle)\|^2 + \|P_{acc} U_{x_i} (|\phi_i\rangle - |\phi'_i\rangle)\|^2 + \|P_{rej} U_{x_i} (|\phi_i\rangle - |\phi'_i\rangle)\|^2. \quad (3)$$

(3) Since the inequality** $\| |\xi_1\rangle \|^2 - \| |\xi_2\rangle \|^2 \leq 2\| |\xi_1\rangle - |\xi_2\rangle \|^2$ holds, we obtain

$$\begin{aligned} 2 \sum_{i=1}^n \|P_{acc} U_{x_i} (|\phi_i\rangle - |\phi'_i\rangle)\|^2 &\geq 2 \sum_{i=1}^n \| \|P_{acc} U_{x_i} |\phi_i\rangle\| - \|P_{acc} U_{x_i} |\phi'_i\rangle\| \|^2 \\ &\geq \sum_{i=1}^n \| \|P_{acc} U_{x_i} |\phi_i\rangle\|^2 - \|P_{acc} U_{x_i} |\phi'_i\rangle\|^2 \| = \left\| \sum_{i=1}^n (\alpha_i - \alpha'_i) \right\|. \end{aligned}$$

**This is shown as follows. Let $|\xi_2\rangle = \alpha|\xi_1\rangle + \beta|\eta\rangle$, where $|\eta\rangle$ is a unit vector that is orthogonal to $|\xi_1\rangle$ and α, β are complex numbers. We then have $\| |\xi_1\rangle - |\xi_2\rangle \|^2 = \| (1 - \alpha)|\xi_1\rangle - \beta|\eta\rangle \|^2 = |1 - \alpha|^2 \| |\xi_1\rangle \|^2 + |\beta|^2$. However, $\| |\xi_1\rangle \|^2 - \| |\xi_2\rangle \|^2 = |1 - \alpha|^2 \| |\xi_1\rangle \|^2 - |\beta|^2$. Since $2|1 - \alpha|^2 \geq |1 - \alpha|^2$, we obtain the desired inequality.

In a similar manner, it follows that $2 \sum_{i=1}^n \|P_{rej} U_{x_i}(|\phi_i\rangle - |\phi'_i\rangle)\|^2 \geq |\sum_{i=1}^n (\beta_i - \beta'_i)|$. Therefore, (2) implies

$$\begin{aligned} \||\phi\rangle - |\phi'\rangle\|^2 &= \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + \sum_{i=1}^n \|P_{acc} U_{x_i}(|\phi\rangle - |\phi'\rangle)\|^2 + \sum_{i=1}^n \|P_{rej} U_{x_i}(|\phi\rangle - |\phi'\rangle)\|^2 \\ &\geq \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + \frac{1}{2} \left| \sum_{i=1}^n (\alpha_i - \alpha'_i) \right| + \frac{1}{2} \left| \sum_{i=1}^n (\beta_i - \beta'_i) \right|. \end{aligned}$$

(4) Since $U_{x_i}^\dagger U_{x_i} = I$, we obtain

$$\langle \phi_i | \phi'_i \rangle = \langle \phi_i | U_{x_i}^\dagger U_{x_i} | \phi'_i \rangle = \langle \phi_i | T_{x_i}^\dagger T_{x_i} | \phi'_i \rangle + \langle \phi_i | U_{x_i}^\dagger P_{acc} U_{x_i} | \phi'_i \rangle + \langle \phi_i | U_{x_i}^\dagger P_{rej} U_{x_i} | \phi'_i \rangle. \quad (4)$$

Using this equality together with Eq.(2) and the inequality $|\langle \xi | \xi' \rangle| \leq \|\xi\| \|\xi'\|$, we obtain

$$\begin{aligned} |\langle \phi_i | \phi'_i \rangle - \langle \phi_i | T_{x_i}^\dagger T_{x_i} | \phi'_i \rangle| &\leq |\langle \phi_i | U_{x_i}^\dagger P_{acc} U_{x_i} | \phi'_i \rangle| + |\langle \phi_i | U_{x_i}^\dagger P_{rej} U_{x_i} | \phi'_i \rangle| \\ &\leq \|P_{acc} U_{x_i} | \phi_i \rangle\| \|P_{acc} U_{x_i} | \phi'_i \rangle\| + \|P_{rej} U_{x_i} | \phi_i \rangle\| \|P_{rej} U_{x_i} | \phi'_i \rangle\| \\ &\leq \frac{1}{2} [(\|P_{acc} U_{x_i} | \phi_i \rangle\|^2 + \|P_{rej} U_{x_i} | \phi_i \rangle\|^2) + (\|P_{acc} U_{x_i} | \phi'_i \rangle\|^2 + \|P_{rej} U_{x_i} | \phi'_i \rangle\|^2)] \\ &= \frac{1}{2} [(\||\phi_i\rangle\|^2 - \|T_{x_i} | \phi_i \rangle\|^2) + (\||\phi'_i\rangle\|^2 - \|T_{x_i} | \phi'_i \rangle\|^2)] \\ &= \frac{1}{2} [(\||\phi_i\rangle\|^2 - \||\phi_{i+1}\rangle\|^2) + (\||\phi'_i\rangle\|^2 - \||\phi'_{i+1}\rangle\|^2)], \end{aligned}$$

where the last inequality follows from Cauchy-Schwartz inequality. Hence, we obtain

$$\begin{aligned} |\langle \phi | \phi' \rangle - \langle \phi | T_x^\dagger T_x | \phi' \rangle| &= \left| \sum_{i=1}^n (\langle \phi_i | \phi'_i \rangle - \langle \phi_i | T_{x_i}^\dagger T_{x_i} | \phi'_i \rangle) \right| \leq \sum_{i=1}^n |\langle \phi_i | \phi'_i \rangle - \langle \phi_i | T_{x_i}^\dagger T_{x_i} | \phi'_i \rangle| \\ &= \frac{1}{2} \sum_{i=1}^n [(\||\phi_i\rangle\|^2 - \||\phi_{i+1}\rangle\|^2) + (\||\phi'_i\rangle\|^2 - \||\phi'_{i+1}\rangle\|^2)] \\ &= \frac{1}{2} [(\||\phi_1\rangle\|^2 - \||\phi_{n+1}\rangle\|^2) + (\||\phi'_1\rangle\|^2 - \||\phi'_{n+1}\rangle\|^2)] \\ &= \frac{1}{2} [(\||\phi\rangle\|^2 - \|T_x | \phi \rangle\|^2) + (\||\phi'\rangle\|^2 - \|T_x | \phi' \rangle\|^2)], \end{aligned}$$

where the last equality comes from $|\phi_{n+1}\rangle = T_x | \phi \rangle$ and $|\phi'_{n+1}\rangle = T_x | \phi' \rangle$. \square

Now, we are ready to prove Lemma 3.1.

Proof of Lemma 3.1(1): A simple calculation shows

$$\begin{aligned} \||\phi\rangle - |\phi'\rangle\|^2 - \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 &= (\||\phi\rangle\|^2 - \|T_x | \phi \rangle\|^2) + (\||\phi'\rangle\|^2 - \|T_x | \phi' \rangle\|^2) \\ &\quad + (\langle \phi | T_x^\dagger T_x | \phi' \rangle + \langle \phi' | T_x^\dagger T_x | \phi \rangle - \langle \phi | \phi' \rangle - \langle \phi' | \phi \rangle) \\ &\leq (\||\phi\rangle\|^2 - \|T_x | \phi \rangle\|^2) + (\||\phi'\rangle\|^2 - \|T_x | \phi' \rangle\|^2) \\ &\quad + |\langle \phi | T_x^\dagger T_x | \phi' \rangle - \langle \phi | \phi' \rangle| + |\langle \phi' | T_x^\dagger T_x | \phi \rangle - \langle \phi' | \phi \rangle|. \end{aligned}$$

Combining the above inequality with Claim 11(4), we then obtain the desired consequence.

Proof of Lemma 3.1(2): Recall that $\psi = (|\phi\rangle, \gamma_1, \gamma_2)$ and $\psi' = (|\phi'\rangle, \gamma'_1, \gamma'_2)$. First, we note that

$$\begin{aligned} (\|\psi\| + \|\psi'\|)^2 &= \|\psi\|^2 + 2\|\psi\| \|\psi'\| + \|\psi'\|^2 \\ &\geq \||\phi\rangle\|^2 + \||\phi'\rangle\|^2 + 2\||\phi\rangle\| \||\phi'\rangle\| + |\gamma_1| + |\gamma'_1| + |\gamma_2| + |\gamma'_2| \end{aligned}$$

because $\|\psi\| \geq \||\phi\rangle\|$ and $\|\psi'\| \geq \||\phi'\rangle\|$. Using the above inequality, we obtain

$$\begin{aligned} \|\psi + \psi'\|^2 &= \||\phi\rangle + |\phi'\rangle\|^2 + |\gamma_1 + \gamma'_1| + |\gamma_2 + \gamma'_2| \\ &\leq \||\phi\rangle\|^2 + \||\phi'\rangle\|^2 + |\langle \phi | \phi' \rangle| + |\langle \phi' | \phi \rangle| + |\gamma_1| + |\gamma'_1| + |\gamma_2| + |\gamma'_2| \\ &\leq \||\phi\rangle\|^2 + \||\phi'\rangle\|^2 + 2\||\phi\rangle\| \||\phi'\rangle\| + |\gamma_1| + |\gamma'_1| + |\gamma_2| + |\gamma'_2| \\ &\leq (\|\psi\| + \|\psi'\|)^2, \end{aligned}$$

where the second inequality follows from the fact that $|\langle \phi | \phi' \rangle| \leq \||\phi\rangle\| \||\phi'\rangle\|$.

Proof of Lemma 3.1(3): When we apply \hat{T}_{x_1} to ψ , we obtain $\hat{T}_{x_1}\psi = (T_{x_1}|\phi\rangle, \gamma_1 + \|P_{acc}U_{x_1}|\phi\rangle\|^2, \gamma_2 + \|P_{rej}U_{x_1}|\phi\rangle\|^2)$. Similarly, applying $\hat{T}_{x_1x_2}$ to ψ , we obtain $\hat{T}_{x_1x_2}\psi = (T_{x_1x_2}|\phi\rangle, \gamma_1 + \sum_{i=1}^2 \|P_{acc}U_{x_i}|\phi_i\rangle\|^2, \gamma_2 + \sum_{i=1}^2 \|P_{rej}U_{x_i}|\phi_i\rangle\|^2)$. In the end, we obtain $\hat{T}_x\psi = (T_x|\phi\rangle, \gamma_1 + \sum_{i=1}^n \alpha_i, \gamma_2 + \sum_{i=1}^n \beta_i)$. A similar reasoning shows that $\hat{T}_x\psi' = (T_x|\phi'\rangle, \gamma'_1 + \sum_{i=1}^n \alpha'_i, \gamma'_2 + \sum_{i=1}^n \beta'_i)$.

Now, let us consider $\|\hat{T}_x\psi - \hat{T}_x\psi'\|$, which equals

$$\|\hat{T}_x\psi - \hat{T}_x\psi'\|^2 = \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + \left| \gamma_1 - \gamma'_1 + \sum_{i=1}^n \alpha_i - \sum_{i=1}^n \alpha'_i \right| + \left| \gamma_2 - \gamma'_2 + \sum_{i=1}^n \beta_i - \sum_{i=1}^n \beta'_i \right|. \quad (5)$$

A simple observation of the above equality leads to

$$\|\hat{T}_x\psi - \hat{T}_x\psi'\|^2 \leq \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + |\gamma_1 - \gamma'_1| + |\gamma_2 - \gamma'_2| + \left| \sum_{i=1}^n (\alpha_i - \alpha'_i) \right| + \left| \sum_{i=1}^n (\beta_i - \beta'_i) \right|.$$

Since $\psi - \psi' = (|\phi\rangle - |\phi'\rangle, \gamma_1 - \gamma'_1, \gamma_2 - \gamma'_2)$, it holds that $\|\psi - \psi'\|^2 = \| |\phi\rangle - |\phi'\rangle \|^2 + |\gamma_1 - \gamma'_1| + |\gamma_2 - \gamma'_2|$. Hence, from the above inequality together with Claim 11(3), we conclude:

$$\begin{aligned} 2\|\psi - \psi'\|^2 &= 2\| |\phi\rangle - |\phi'\rangle \|^2 + 2|\gamma_1 - \gamma'_1| + 2|\gamma_2 - \gamma'_2| \\ &\geq 2\|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + 2|\gamma_1 - \gamma'_1| + 2|\gamma_2 - \gamma'_2| + \left| \sum_{i=1}^n (\alpha_i - \alpha'_i) \right| + \left| \sum_{i=1}^n (\beta_i - \beta'_i) \right| \\ &\geq \|\hat{T}_x\psi - \hat{T}_x\psi'\|^2. \end{aligned}$$

Proof of Lemma 3.1(4): From Eq.(5), it follows that

$$\begin{aligned} &\|\hat{T}_x\psi - \hat{T}_x\psi'\|^2 \\ &\geq \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + \left| \gamma_1 - \gamma'_1 - \sum_{i=1}^n \alpha_i + \sum_{i=1}^n \alpha'_i \right| + \left| \gamma_2 - \gamma'_2 - \sum_{i=1}^n \beta_i + \sum_{i=1}^n \beta'_i \right| \\ &\geq \|T_x(|\phi\rangle - |\phi'\rangle)\|^2 + |\gamma_1 - \gamma'_1| + |\gamma_2 - \gamma'_2| - \left| \sum_{i=1}^n (\alpha_i - \alpha'_i) \right| - \left| \sum_{i=1}^n (\beta_i - \beta'_i) \right|. \end{aligned}$$

Using Claim 11(3) and $\|\psi - \psi'\|^2 = \| |\phi\rangle - |\phi'\rangle \|^2 + |\gamma_1 - \gamma'_1| + |\gamma_2 - \gamma'_2|$, the above inequality immediately implies

$$\|\hat{T}_x\psi - \hat{T}_x\psi'\|^2 \geq \|\psi - \psi'\|^2 - 3\| |\phi\rangle - |\phi'\rangle \|^2 + 3\|T_x(|\phi\rangle - |\phi'\rangle)\|^2.$$

References

- [1] S. Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 1 (2005) 1–28.
- [2] A. Ambainis and R. Freivalds. 1-way quantum finite automata: strengths, weaknesses, and generalizations. In *Proc. 39th Annual Symposium on Foundations of Computer Science*, pp.332–342, 1998.
- [3] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM*, 49 (2002), 496–511.
- [4] A. Brodsky and N. Pippenger. Characterizations of 1-way quantum finite automata. *SIAM J. Comput.*, 31 (2002) 1456–1478.
- [5] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*, (Second Edition). Addison Wesley, 2001.
- [6] R. M. Karp and R. Lipton. Turing machines that take advice. *L'Enseignement Mathématique*, 2nd series, 28 (1982) 191–209.
- [7] A. Kondacs and J. Watrous. On the power of quantum finite state automata. In *Proc. 38th Annual Symposium on Foundations of Computer Science*, pp.66–75, 1997.

- [8] C. Moore and J. Crutchfield. Quantum automata and quantum languages. *Theor. Comput. Sci.*, 237 (2000) 275–306.
- [9] P. Michel. An NP-complete language accepted in linear time by a one-tape Turing machine. *Theor. Comput. Sci.*, 85 (1991) 205–212.
- [10] H. Nishimura and T. Yamakami. Polynomial-time quantum computation with advice. *Inf. Process. Lett.*, 90 (2004) 195–204.
- [11] H. Nishimura and T. Yamakami. An application of quantum finite automata to interactive proof systems. *J. Comput. System Sci.*, 75 (2009) 255–269. A preliminary version appeared in *Proc. 9th International Conference on Implementation and Application of Automata*, Lecture Notes in Computer Science, Vol.3317, pp.225–236, Springer, 2004.
- [12] R. Raz. Quantum Information and the PCP Theorem. *Algorithmica*, 55 (2009) 462–489.
- [13] K. Tadaki, T. Yamakami, and J. C. H. Lin. Theory of one-tape linear-time Turing machines. *Theor. Comput. Sci.*, 411 (2010) 22–43. A preliminary version appeared in *Proc. 30th SOFSEM Conference on Current Trends in Theory and Practice of Computer Science*, Lecture Notes in Computer Science, Vol.2932, pp.335–348, Springer, 2004.
- [14] T. Yamakami. Swapping lemmas for regular and context-free languages. Available at arXiv:0808.4122, 2008.
- [15] T. Yamakami. The roles of advice to one-tape linear-time Turing machines and finite automata. *Int. J. Found. Comput. Sci.*, 21 (2010) 941–962. An early version appeared in the *Proc. 20th International Symposium on Algorithms and Computation*, Lecture Notes in Computer Science, Vol.5878, pp.933–942, Springer, 2009.
- [16] T. Yamakami. Immunity and pseudorandomness of context-free languages. *Theor. Comput. Sci.*, 412 (2011) 6432–6450.
- [17] T. Yamasaki, H. Kobayashi, and H. Imai. Quantum versus deterministic counter automata. *Theor. Comput. Sci.* 334 (2005) 275–297.